נושאים בתורת הקודים מתקני שגיאות - 80868

15 בינואר 2013

מרצים: פרופ' אלכס לובוצקי וד"ר טלי קאופמן

הערות יתקבלו בברכה - noga.rotman@gmail.com. אהבתם? יש עוד!
http://bit.ly/integrali

תוכן עניינים

1 הקדמה והגדרות בסיסיות 3
2 קודים ציקליים 8
2.1 קודי $Reed - Solomon$ 8
2.2 איך חושבים על קוד ציקלי באופן אלגברי 11
2.3 קודים בפולינומים רב־משתנים $(Reed - Muller\ Codes)$ 12
2.4 קודי BCH 13
2.5 דיון ראשון - האם יש קודים ציקליים טובים? 16
2.5.1 $Quadratic\ Residue\ Code$ 16
2.6 עקרון אי הוודאות 17
2.6.1 חבורות אבליות סופיות 17
2.6.2 עקרון אי הוודאות עבור פולינום ב־$\mathbb{C}[x]$ 21
2.6.3 עקרון אי הוודאות בשדות סופיים, והקשר לקודים ציקליים טובים 26
2.6.4 מה צריך להוכיח בתורת המספרים כדי לקבל קודים ציקליים טובים? 28
2.7 קודים דואליים לקודי BCH, קודי האדמר ואפליקציות 29
3 גרפים וקודים 29
3.1 מקודים לגרפים 30
3.1.1 ניתוח תכונות הקוד 31
3.2 קודים סימטריים 35
4 קודים בדיקים מקומית (LTC - Locallty Testable Codes) 37

1 הקדמה והגדרות בסיסיות

23/10/2012

אזהרה: מי שחושב שיצא מכאן יודע תורת הקודים - אין זה נכון! אין זה קורס סטנדרטי הלומד את הנושא באופן שיטתי, אלא נושאים שמעניינים את המרצים מתמטית.

עקרונית, הבעיה היא הנדסית - יש משגר הודעה (מקודד) ומקבל הודעה (מפענח). הודעה מבחינתנו היא סדרה ארוכה של בדר"כ 0 ו-1 (עם זאת, נדבר בהמשך על שדות אחרים), כלומר מבקשים לשדר וקטור מעל השדה $\mathbb{F}_2^k$. אם ישלח את ה-k ביטים כפי שהם ותיפול טעות בחלק מהם, המקבל לא ידע כיצד לתקן. על כן במקום זאת, המשגר הופך את הוקטור ה-k מימדי לוקטור ארוך יותר n-מימדי, ושולח אותו. כלומר, ישנה העתקה:

$$T : \mathbb{F}_2^k \to \mathbb{F}_2^n$$

ובמקום לשלוח וקטור $\mathbb{F}_2^k \ni \alpha$, ישלח $\mathbb{F}_2^n \ni T\alpha$, ונצפה מ-$T$ שהיא תהיה שיטה אשר בעזרתה המקבל יוכל לתקן את השגיאות שנפלו בדרך.

שיטה ראשונה ופשוטה: נשלח כל ביט שלוש פעמים.

מה הבעיה בשיטה הזו? מצד אחד, יש כאן בזבוז גדול - מגדילים את אורך ההודעה פי שלוש. מצד שני, מרוויחים ממנה מעט - אפשר לתקן רק שגיאות רחוקות זו מזו, אחרת ה"תיקון" יהיה שגוי.

כל התורה היא מציאת T שכזו המשכנת את המרחב $\mathbb{F}_2^k$ ב-$\mathbb{F}_2^n$ באופן נוח לשימוש (קידוד ופיענוח), למשל פונקציה לינארית, וכמו כן שמקדם היעילות, כלומר היחס בין n ל-k, יהיה גבוה.

איך מתקנים שגיאות?

נסתכל במילות הקוד החוקיות - הטווח $T\left(\mathbb{F}_2^k\right)$ - זוהי קבוצת וקטורים ב-$\mathbb{F}_2^n$.

נניח ש-$d > dist(T\alpha, T\beta)$ לכל $\alpha, \beta \in \mathbb{F}_2^k$, כאשר עבור וקטור $v \in (v_1, ..., v_m) = v$, $\mathbb{F}_q^m$, נגדיר:

$$(Hamming)\ \ wt(v) = \#\{i | v_i \neq 0\} = \|v\|$$
$$\Rightarrow v, w \in \mathbb{F}_q^m,\ \ dist(v, w) := wt(v - w) = \#\{i | v_i \neq w_i\}$$

תרגיל: $dist$ הוא מטריקה על $\mathbb{F}_q^m$, כלומר:

$$dist(\alpha, \beta) = dist(\beta, \alpha)$$
$$dist(\alpha, \beta) = 0 \Leftrightarrow \alpha = \beta$$
$$dist(\alpha, \gamma) \leq dist(\alpha, \beta) + dist(\beta, \gamma)$$

אם נביט בכדורים:

$$B_r(w) = \{v | dist(w, v) \leq r\}$$

ההנחה $d < dist(T\alpha, T\beta)$ לכל $\alpha, \beta \in \mathbb{F}_2^k$, פרושה כי

$$B_{\frac{d}{2}}(T\alpha) \bigcap B_{\frac{d}{2}}(T\beta) = \phi$$

כלומר כל הכדורים האלו הן זרים. לכן, אם בשידור נפלו פחות מ-$\frac{d}{2}$ שגיאות, אזי "נפענח" את הוקטור שהתקבל לאותו $T\alpha$ הקרוב אליו (והוא יחיד תחת ההנחה!). אם נפלו יותר מ-$\frac{d}{2}$

שגיאות, כלומר הרשת ממש "מלוכלכת", אז פעולת התיקון לא עוזרת, לכן נעבוד ברשתות שנוכל להניח עליהן מספר מסויים של שגיאות.

כאמור אנו מחפשים n קטן ככל אפשר, ועם זאת היכולת לתקן כמה שיותר שגיאות. ברור אינטואיטיבית כי שתי המטרות הללו סותרות אחת את השניה, על כן יש למצוא איזון בין השתיים. האומנות אם כך של קודים מתקני שגיאות היא מציאת פשרות בין שתי הדרישות הללו.

בקודים הראשונים הקלאסיים למשל היו שולחים $k+1$ ביטים, כאשר הביט הנוסף הוא ה־XOR של הקודמים לו. אם נפלה טעות אחת, נדע כי נפלה שגיאה, אך לא נדע היכן (אולי נפלה בכלל בביט האחרון, ואז השאר נכון?). אם נפלו שתי שגיאות, כבר לא נדע שיש שגיאה (ה־XOR ישאר נכון). אם יודעים ששגיאות הן מאוד נדירות אפשר לשדר כך, ובמידה ונפלה שגיאה אפשר לשדר שוב. בדר"כ זה לא מספיק[1].

המתמטיקאים בדר"כ התייחסו לנושא עבור n שואף לאינסוף. במקרה זה היו קודים "גרועים" כאשר n שואף לאינסוף, אך השתמשו בהם בכל מקום כי הקוד היה טוב ל־n קטן כלשהוא. עם זאת, עם ההתפתחות הטכנולוגית, n גדל יותר ויותר.

נעבור על ההגדרות באופן ריגורוזי ונסקור תוצאות קלאסיות פשוטות.

הגדרה 1.1 יהי $\mathbb{F}_q$ שדה סופי מסדר q. "קוד" זו העתקה חח"ע:

$$T : \mathbb{F}_q^k \to \mathbb{F}_q^n$$

התמונה $C := T\left(\mathbb{F}_q^k\right)$ = מילות הקוד.
הקצב $(rate)$ של הקוד הוא $\frac{k}{n}$.
המרחק $(distance)$ של הקוד הוא:

$$min\left\{dist\left(T\alpha, T\beta\right)|\alpha \neq \beta \in \mathbb{F}_q^k\right\}$$

T כזו תסומן ב־$(n,k,d)_q$. n נקרא אורך הקוד, k נקרא מימד הקוד, ו־d הוא מרחק הקוד.
אם $T : \mathbb{F}_q^k \to \mathbb{F}_q^n$ העתקה לינארית נאמר שזה קוד לינארי, ויסומן:

$$[n,k,d]_q$$

הערה 1.2 בהחלט היה מקום בעת קביעת איכות הקוד לדון באלגוריתם הקידוד ובאלגוריתם הפענוח ובמהירותם ־ זהו לא עניין טריוויאלי בכלל. עם זאת, לא נדון בקורס זה באלגוריתמיקה.

הערה 1.3 בקוד לינארי $C = T\left(\mathbb{F}_2^k\right)$ הוא תת מרחב, וכן:

$$dist\left(C\right) = min\left\{wt\left(\gamma\right)|0 \leq \gamma \in C\right\}$$

הוכחה:

$$dist\left(C\right) = min\left\{dist\left(T\alpha, T\beta\right)|\, \alpha \neq \beta \in C\right\} = \left\{\|\alpha - \beta\||\, \alpha \neq \beta \in C\right\}$$

כלומר כל וקטור הוא המרחק שלו מאפס, ואז:

$$\left\{\|\alpha - \beta\||\, \alpha \neq \beta \in C\right\} = min\left\{wt\left(\gamma\right)|0 \leq \gamma \in C\right\}$$

■

[1] גם למרצים גם לא ממש ידוע מה מספיק היום ומה לא ־ אנחנו נעסוק בעניין המתמטי.

הגדרה 1.4 משפחה של קודים $C_i = (n_i, k_i, d_i)_{q_i}$ תקרא משפחה טובה אסימפטוטית אם קיים $\varepsilon > 0$ כך ש: $\frac{k_i}{n_i} \geq \varepsilon$, וגם $\frac{d_i}{n_i} \geq \varepsilon$.

בהמשך, כאשר נגיד "קוד טוב", נתכוון למשפחה של קודים טובה אסימפטוטית.
זה בכלל לא טריוויאלי שקודים טובים קיימים.
נניח $q = 2$. נסמן ב־$V(n,r)$ את נפח כדור ברדיוס r ב־$\mathbb{F}_2^n$, כלומר:

$$V(n,r) = \#\{\alpha \in \mathbb{F}_2^n | \, dist(\alpha, 0) \leq r\} = \sum_{i=0}^{k} \begin{pmatrix} n \\ i \end{pmatrix}$$

משפט 1.5 לכל d ולכל n מספיק גדול קיים קוד C ב־$\mathbb{F}_2^n$ עם $dist(C) \geq d$, ו:

$$|C| \geq \frac{2^n}{V(n,d)}$$

יתר על כן, קיים אפילו קוד לינארי כזה.

משפט 1.6 כל קוד מאורך n ומרחק d, מקיים:

$$|C| \leq \frac{2^n}{V\left(n, \frac{d}{2}\right)}$$

אם נסמן $\delta = \frac{d}{2}$=המרחק המנורמל, אפשר להניח ש־$\delta \leq \frac{1}{2}$, אז:

$$\begin{pmatrix} n \\ \delta n \end{pmatrix} \leq V(n,d) = \sum_{i=0}^{\delta n} \begin{pmatrix} n \\ i \end{pmatrix} \leq n \cdot \begin{pmatrix} n \\ \delta n \end{pmatrix}$$

נסמן את פונקציית האנטרופיה:

$$H(\delta) = -\delta log_2 \delta - (1-\delta) log_2 \delta, \;\; 0 < \delta < 1$$

תרגיל: $\begin{pmatrix} n \\ \delta n \end{pmatrix} \sim 2^{H(\delta)n}$, $\frac{log\begin{pmatrix} n \\ \delta n \end{pmatrix}}{H(\delta)n} \to 1$ (הוכחה: השמה בנוסחאת סטרלינג).
לא להבהל - זהו רק שינוי בסימנים. אנו מחפשים קודים טובים.

מסקנה 1.7 משפט 2 אומר לנו בסימוני אנטרופיה עבור $d = \delta n$ כי:

$$|C| \leq \frac{2^n}{2^{H(\delta)n}} = 2^{(1-H(\delta))n}$$

כלומר, אם $\frac{dist}{n} \geq \delta$, אזי:

$$rate = \frac{k}{n} \leq 1 - H\left(\frac{\delta}{2}\right)$$

מסקנה 1.8 משפט 1 אומר שאפשר להגיע לא כל כך רחוק מזה: לכל $\delta \leq \frac{1}{2}$ ו־n מספיק גדול, קיים קוד לינארי עם מרחק מנורמל δ כך ש:

$$\frac{k}{n} \geq 1 - H(\delta)$$

כעת ־ נוכיח את המשפטים: **הוכחה: משפט 1**: נראה מעין אלגוריתם שבונה את הקוד הנדרש (הקוד שנקבל אינו לינארי). הוא לא יעיל (זמן ריצה אקספוננציאלי), אבל אין לנו כאן דרישה שכזו.

נבנה קוד שעומד בתנאים: נתחיל ב־$C = \phi$, ובכל שלב נכניס וקטור נוסף ל־C עד שנתקע ונעצר. לא נתקע עד שנקבל מספיק איברים, וכן נקבל את המרחק הרצוי.

נתחיל ב־$V = \mathbb{F}_2^q$, ו־$C = \phi$.

צעד האלגוריתם: נכניס וקטור $x \in V$ לתוך C, ונוציא מ־V (ונזרוק החוצה) כל איבר ב־V שמרחקו מ־x קטן־שווה d. נחזור על הפעולה עד שנתקע.

התהליך נמשך עד שכל איברי V נפסלו "לבוא בקהל". בכל הכנסת איבר חדש, פוסלים לכל היותר[2] $V(n,d)$ איברים. לכן האלגוריתם לא יתקע לפני שהוא יבצע $\frac{2^n}{V(n,d)}$ צעדים, וזה מוכיח את משפט 1 לקוד לא לינארי. בשיעור הבא נראה מדוע אפשר לקבל גם קוד לינארי.

משפט 2: אם $|C| = c$, אז יש לנו c וקטורים ב־$\mathbb{F}_2^n$ שהכדורים ברדיוס $\frac{d-1}{2}$ סביבם זרים, ולכן:

$$c \cdot V\left(n, \frac{d-1}{2}\right) \leq 2^n \Rightarrow |C| \leq \frac{2^n}{V\left(n, \frac{d-1}{2}\right)}$$

■

30/10/2012

לא הוכחנו שקיים קוד לינארי טוב ־ נראה זאת עכשיו:

משפט 1.9 קיים קוד לינארי C ב־$\mathbb{F}_2^n$ עם $distance = d$, ו־$2^{dim(C)} = |C| \geq \frac{2^n}{V(n,d)}$.

הערה 1.10 נזכיר כי קוד הוא $C \subseteq \mathbb{F}_2^n$, וקוד לינארי $C \leq \mathbb{F}_2^n$. המרחק מוגדר להיות:

$$dist(C) = min\{dist(\alpha, \beta) \,|\alpha \neq \beta \in C\}$$

ואם C לינארי, אזי:

$$dist(C) = min\{\|\alpha\| \,|0 \neq \alpha \in C\}$$

וכמו כן הגדרנו:

$$rate = \frac{log|C|}{log\left(\mathbb{F}_q^n\right)}$$

[2] יתכן וחלק נפסלו בשלב קודם.

מסקנה 1.11 יש קודים לינאריים טובים, ז"א קיים $\varepsilon > 0$, $\{C_n\}_{n\to\infty}$, כך ש:

$$\frac{dist\,(C)}{n}, \frac{dim\,(C)}{n} \geq \varepsilon$$

(לכל $\delta < \frac{1}{2}$ קיים $\delta' > 0$ וקיימים קודים C_n כך ש: $dist\,(C_n) \geq \delta n,\ dim\,(C_n) \geq \delta' n$).

נוכיח את המשפט: **הוכחה:** קוד $C \geq \mathbb{F}_2^n$ נקבע ע"י בחירת בסיס ל־C, או ע"י הצגת C כגרעין של טרנספורמציה לינארית A:

$$C = \left\{x \in \mathbb{F}_2^n | Ax = \overrightarrow{0}\right\},\ A = (m \times n)$$

הגדרה 1.12 A נקראת מטריצת בדיקת זוגיות - parity check.

נניח A היא מטריצת ה־parity check של C = $kerA$.

למה 1.13 $dist\,(C)$ = המספר המינימלי של עמודות של A שסכומן 0.

הוכחה: אם $\sum_{j=1}^{s} \gamma_{i_s} = 0$ כאשר $\gamma_{i_1}, ..., \gamma_{i_s}$ עמודות של A, אזי הוקטור שרכיביו 1 במקומות $\{i_1, ..., i_s\}$ ו־0 אחרת הוא ב־C, כלומר $dist\,(C) \leq s$. מצד שני, נניח יש ב־C וקטור ממשקל t ורכיביו השונים מ־0 הם במקומות $i_1, ..., i_t$. אזי ברור ש: $\sum_{l=1}^{t} \gamma_{i_l} = 0$, ולכן $t \leq s$.נבנה עכשיו את המטריצה A

עמודה אחר עמודה, תוך כדי הבטחה שלא יהיו פחות מ־d עמודות שסכומן 0. יהי m פרמטר שיקבל אח"כ.

ניתן לבחור את הוקטור ה־j־אי בתהליך כל הזמן ש:

$$(*) \sum_{r<d} \begin{pmatrix} j-1 \\ r \end{pmatrix} < 2^m$$

שכן ניתן לבחור כל עוד הוקטור החדש אינו סכום של אף תת קבוצה בגודל r וקטורים (לכל $r < d$) מתוך קבוצת הוקטורים שנבחרו עד כה.

אנו רוצים להיות מסוגלים להמשיך בתהליך עד שנגיע ל־$j = n$.

תנאי $(*)$ מתקיים אוטומטית לכל $j \leq n$ אם מתקיים ל־$j = n$. מה זה אומר על m אם צריך ש:

$$(**) \sum_{r<d} \begin{pmatrix} n-1 \\ r \end{pmatrix} < 2^m$$

נבחר את ה־m הקטן ביותר שעדיין $(**)$ מתקיים. מיהו?

$$2^{m-1} \leq \overbrace{\sum_{r<d} \begin{pmatrix} n-1 \\ r \end{pmatrix}}^{(***)} < 2^m$$

נשים לב כי $(***)$ הוא $\#B_{n-1}(d-1)$ = הנפח של כדור ברדיוס $d-1$ ב־$\mathbb{F}_2^{n-1}$. אם נבחר נכון את m, אזי $dim(C) \geq n-m$.

$$\Rightarrow |C| \geq \frac{2^n}{2^m} \geq \frac{2^n}{2V(n-1,d-1)} \sim \frac{2^n}{V(n,d)}$$

■

■

2 קודים ציקליים

2.1 קודי $Reed-Solomon$

חסם הסינגלטון:

למה 2.1 לכל $\mathbb{F}_q^n \geq C$ עם $dim(C)=k$, מתקיים $d=dist(C) \leq n-(k-1)$.
כלומר, $dim(C)+dist(C) \leq n-1$.

הלמה בעצם נותנת חסם "על כמה קוד יכול להיות טוב". **הוכחה:** נניח $dim(C)=k$, ונשליך את כל איברי C ל־$(k-1)$ הקואורדינטות הראשונות. לפי עקרון שובך היונים יש $\alpha \neq \beta \in C$ כך ש־$(k-1)$ הקואורדינטות הראשונות הן שוות, ולכן:

$$dist(\alpha,\beta) \leq n-(k-1)$$

■

הגדרה 2.2 יהי $\mathbb{F}=\mathbb{F}_q$ שדה סופי, $\alpha_1,...,\alpha_n$ איברים שונים של $\mathbb{F}$ (בפרט $q \geq n$). בהנתן $k \leq n\,(\leq q)$, נגדיר קוד $T:\mathbb{F}_q^k \to \mathbb{F}_q^n$:

$$T(a_0,...,a_{k-1}) = \left(...,\sum_{i=0}^{k-1} a_i\alpha_j^i,...,\sum_{i=0}^{k-1} a_i\alpha_n^i\right)$$

כלומר התייחסנו לפולינום שנוצר ע"י ה־k־איה, והצבנו בו את האיברים $\alpha_1,...,\alpha_n$.

T היא העתקה לינארית, והמטריצה המייצגת אותה היא ון־דר־מונדה הנראית כך:

$$\begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{k-1} \\ \vdots & & & & \vdots \\ 1 & \alpha_n & \cdots & \cdots & \alpha_n^{k-1} \end{pmatrix}$$

T היא חח"ע - שכן אם $T(f_1)=T(f_2)$, יש לנו שני פולינומים ממעלה $\geq n-1$ המתלכדים על n איברים ולכן הם שווים.

טענה 2.3

$$dist(C) = d = n+1-k$$

הוכחה: מאחר ו־C קוד לינארי, $dist\left(C\right)=\underset{0\neq\beta\in C}{min}\left\{\left\|\beta\right\|\right\}$, $\left\|\beta\right\|=\#\left\{i|\beta_i\neq 0\right\}$.

אם $\beta\in C$ אזי $\beta=T\left(f\left(x\right)\right)$ ו־$deg\left(f\left(x\right)\right)\leq k-1$, ולכן $f\left(x\right)$ מתאפס על לכל היותר $k-1$ מתוך ה־α_i־אים, ולכן לא מתאפס על $n-\left(k-1\right)$, ולכן $\left\|\beta\right\|\geq n+1-k$. ■

שיטת Justemsen

נניח $\mathbb{F}_{q^l}$ הרחבה סופית של $\mathbb{F}_q$.

סימון: נקבל $0\neq\alpha\in\mathbb{F}_{q^l}$, ונגדיר קוד $C_2\leq\mathbb{F}_{q^l}\times\mathbb{F}_{q^l}\simeq\mathbb{F}_q^{2l}$ ע"י:

$$\begin{aligned}&\tilde{\alpha}:\mathbb{F}_{q^l}\to\mathbb{F}_{q^l}\times\mathbb{F}_{q^l}\\&\beta\to\left(\beta,\alpha\cdot\beta\right)\end{aligned}$$

נחשוב על $C_\alpha=Im\left(\tilde{\alpha}\right)$ כתת מרחב (קוד) של $\mathbb{F}_q^{2l}$.

טענה 2.4 לכל $\varepsilon>0$, לכמעט כל $0\neq\alpha\in\mathbb{F}_{q^l}$, C_α הוא: $\left[2l,l,H_q^{-1}\left(\frac{1}{2}-\varepsilon\right)\cdot 2l\right]_q$ קוד לינארי.

הערה 2.5 שני הפרמטרים הראשונים טריוויאלים, מה שנשאר להוכיח הוא המרחק, כאשר:

$$H_q\left(x\right)=-xlog_q\left(x\right)-\left(1-x\right)log_q\left(1-x\right),\ 0<x<1$$

כלונר, לאחר שנוכיח נקבל כי כאשר $l\to\infty$, $rate=\frac{l}{2l}=\frac{1}{2}$. זוהי דרך אחרת להוכיח הוכחה של משפחה של קודים טובים.

אבל זו רמאות, כי זה תהליך מקרי, ולא בניה אפקטיבית.

הוכחה: נטען שאם $\alpha_1\neq\alpha_2\in\mathbb{F}_{q^l}^*$, אזי $C_{\alpha_1}\cap C_{\alpha_2}=\left\{0\right\}$. זאת כי אם $\left(\beta,\alpha_1\cdot\beta\right)=\left(\gamma,\alpha_2\cdot\gamma\right)$. זה גורר כי $\beta=\gamma$. אם $\beta=\gamma=0$, סיימנו. אחרת אם $\beta=\gamma\neq 0$, נקבל כי $\alpha_1=\alpha_2$.

נשים לב כי α שמקיימות את התנאי יש q^l כאלה, כלומר נקבל "הרבה מאוד" תת מרחבים כאלה, ומכך נגיע ל"מרחק הגדול" שאנחנו רוצים.

אם ל־C_α מרחק $dist\left(C_\alpha\right)\leq d$, אזי $C_\alpha\cap B\left(0,d\right)\neq\left\{0\right\}$. אזי קיימים לכל היותר $\left|B\left(0,d\right)\right|$ α־אות כך ש־$dist\left(C_\alpha\right)\leq d$ מנוסחאת סטרלינג נקבל:

$$\left|B\left(0,d\right)\right|\sim q^{H_q\left(\frac{d}{2l}\right)\cdot 2l}$$

לכן אם ניקח: $d=\left(H_q^{-1}\left(\frac{1}{2}-\varepsilon\right)\right)\cdot 2l$, נקבל:

$$\begin{aligned}&B\left(0,d\right)\sim q^{H_q\left(H_q^{-1}\left(\frac{1}{2}-\varepsilon\right)\right)\cdot 2l}=q^{\left(\frac{1}{2}-\varepsilon\right)\cdot 2l}\\&\Rightarrow\frac{q^{\left(\frac{1}{2}-\varepsilon\right)\cdot 2l}}{q^l}\overset{l\to\infty}{\longrightarrow}0\end{aligned}$$

כלומר הגודל של הכדור "הרבה יותר קטן" מ־q^l, לכן לרב ה־α־אות לקוד המתאים לא יהיה חיתוך עם הכדור (חיתוך עם הכדור = קוד רע, לכן הוכחנו שיש "הרבה" קודים טובים), כלומר לרב הקודים שהגדרנו ככה יהיה מרחק גדול מ־d. ■

תרגילים - חובה 8 מתוך 10 (בערך), אם מסכמים (סיכום עם השלמות וכו') - 3. 6/11/2012

לפעמים לתרגילים לא יהיה קשר לחומר בכיתה, אלא דברים שצריך להכיר.
תזכורת - קוד ריד־סולומון:
בהנתן שדה $\mathbb{F}$, $\alpha_1, ..., \alpha_n \in \mathbb{F}$ שונים.

$$T : \mathbb{F}^k \to \mathbb{F}^n$$

$$T\left((a_0, a_1, ..., a_{k-1})\right) \to \left(f\left(\alpha_1\right), ..., f\left(\alpha_n\right)\right), \ f = \sum_{i=0}^{k-1} a_i x^i$$

כאשר הקוד הוא $C = Im\left(T\right)$.
נמשיך עם כמה הערות על ריד־סולומון.
מקרה פרטי מקובל מאוד של $R - S$ זה לבחור את $\alpha_1, ..., \alpha_n \in \mathbb{F}$ כאוסף שורשי היחידה ה־n־ים בשדה (ז"א $\{\alpha_1, ..., \alpha_n\} = \{\lambda \in \mathbb{F} | \lambda^n = 1\}$), ומניחים שאכן יש ב־$\mathbb{F}$ n (שונים) כאלו).
לשדה סופי $\mathbb{F} = \mathbb{F}_q$ זה כך אמ"מ $h|q$.

טענה 2.6 במקרה זה, $R - S$ הוא קוד ציקלי.

הגדרה 2.7 קוד $C \subseteq \mathbb{F}^n$ יקרא ציקלי אם לכל $(a_0, ..., a_{n-1}) \in \mathbb{F}^n$, $(a_2, ..., a_n, a_1) \in C \Leftrightarrow (a_1, ..., a_n) \in C$.

במימוש של קודים, זו תכונה טובה, אבל נגיד על זה עוד משהו בהמשך.

טענה 2.8 אם $C \subseteq \mathbb{F}^n$ קוד $R - S$ כך ש־$\alpha_1, ..., \alpha_n$ הם n־שורשי היחידה, אזי C הוא קוד ציקלי.

הוכחה:

$$\{\alpha_1, ..., \alpha_n\} = \left\{1, \lambda, \lambda^2, ..., \lambda^{n-1}\right\}, \ \lambda^n = 1$$

ולכל פולינום $f\left(x\right)$ ממעלה $\geq k-1$, גם $f_\lambda\left(x\right) = f\left(\lambda x\right)$ הוא ממעלה $\geq k-1$. נציב ונקבל:

$$\left(f_\lambda\left(1\right), f_\lambda\left(\lambda\right), ..., f_\lambda\left(\lambda^{n-1}\right)\right) = \left(f\left(\lambda\right), f\left(\lambda^2\right), ..., f\left(\lambda^n\right)\right)$$

ואם $\left(f\left(1\right), ..., f\left(\lambda^{n-1}\right)\right) \in C$, גם ההזזה בקוד, כנדרש. ■

בעיה פתוחה בהנתן שדה סופי $\mathbb{F}$, האם קיימת משפחה של קודים לינאריים ציקליים טובים מעל $\mathbb{F}$?
כלומר, האם יש $\varepsilon > 0$ וסדרה $\{n_i\} \to \infty$ ותתי מרחבים $C_i \leq \mathbb{F}^{n_i}$ כך ש:

$$\frac{dim\left(C_i\right)}{n_i}, \frac{dist\left(C_i\right)}{n_i} \geq \varepsilon$$

ו־C_i סגור תחת סיבוב ציקלי!

מרבית המומחים בתחום חושבים שאין כאלו, פרופ' לובוצקי עם זאת חושב שיש. היום בתחום יש רק תוצאות חלקיות, שבדר"כ אומרות שאין כאלו.

בדר"כ קוד שיש לו סימטריות או אינווריאנטים הוא יותר קל למימוש. קוד חשוב שיהיה מהיר לקידוד ולפענוח, ותכונת הציקליות למשל עוזרת בכך.

הגדרה 2.9 אם $C \leq \mathbb{F}^n$ קוד, נאמר ש־C קוד סימטרי אם קיימת חבורה G הפועלת טרנזיטיבית על הקבוצה $\{1,...,n\}$ (וממילא על $\mathbb{F}^n$) כך ש־C אינווריאנטית לפעולת החבורה.

הערה 2.10 ציקלי = מקרה פרטי של סימטרי.

גם פה היו השערות שאין קודים סימטריים טובים, ולפני שנה פרופ' לובוצקי ודר' קאופמן הפריכו את הטענה.

2.2 איך חושבים על קוד ציקלי באופן אלגברי

נביט בקוד ציקלי (כללי) מעל $\mathbb{F}$, אפשר לחשוב:

$$V = \mathbb{F}^n = \left\{ f(x) = a_0 + a_1 x + ... + a_{n-1} x^{n-1} \right\}$$

ניתן לזהות קבוצה זו את החוג הוקטורי ממימד n:

$$= R = {}^{\mathbb{F}[x]}\!/_{(x^n-1)}$$

והנציגים של הקוסטים הם פולינומים מדרגה $< n$.

קוד ציקלי לינארי הוא תת־קבוצה של R שהוא תת־מרחב וסגור ע"י סיבוב ציקלי ימינה, כלומר סגור ביחס להכפלה ב־x:

$$(a_0, ..., a_{n-1}) \simeq \sum_{i=0}^{n-1} a_i x^i$$

$$x \cdot \sum_{i=0}^{n-1} a_i x^i = \sum_{i=0}^{n-1} a_i x^{i+1}$$

ובחוג זה $x^n = 1$, ולכן הפולינום שקיבלנו:

$$\sum_{i=0}^{n-1} a_i x^{i+1} \overset{R}{\rightsquigarrow} (a_{n-1}, a_0, ..., a_{n-2})$$

מכיוון וגם סגור לחיבור, C הוא אידאל ב־R.

ולהיפך, קוד $R = \mathbb{F}^n \supseteq C$ הוא ציקלי אמ"מ הוא אידאל.

לפי משפט ההתאמה, כל אידאל של R מתקבל מאידאל של $F[x]$ המכיל את האידאל $(x^n - 1)$. מאחר ו־$F[x]$ חוג ראשי, כל אידאל כזה מתקבל מפולינום $g(x)$ כך ש: $g(x) \,|\, x^n - 1$.

אז בעצם אפשר להבין את כל האידאלים הציקליים, ולכאורה הבעיה שהצגנו היא מאוד פשוטה ־ בדוק את כל המחלקים של $x^n - 1$. הבעיה היא אכן מאוד פשוטה, אבל רק במצבים מסויימים. קיבלנו כך תרגום לבעיות בתורת המספרים.

הגדרה 2.11 אם $C \leq \mathbb{F}^n$, נסמן $C^\perp = \{ \beta \in \mathbb{F}^n | \, \langle \beta, \alpha \rangle = 0, \ \forall \alpha \in C \}$ = הקוד הדואלי, כאשר:

$$\alpha = (a_1, .., a_n), \ \beta = (b_1, ..., b_n), \ \langle \beta, \alpha \rangle = \sum_{i=1}^{n} b_i a_i, \ dim C^\perp = n - dim C$$

הערה 2.12 זהירות! יתכן ו־$C \cap C^{\perp} \neq 0$, לפעמים $C = C^{\perp}$ (ואז ל־C קוראים קוד דואלי לעצמו).

טענה 2.13 אם $C \leq \mathbb{F}^n$ קוד ציקלי, גם $C^{\perp}$ קוד ציקלי.

הוכחה: או ישירה מההגדרה, או לבדוק שגם $C^{\perp}$ הוא אידאל. ■

התרגיל שינתן בשבוע הבא:

אם יודעים ש־C הוא קוד ציקלי, אזי הוא נוצר על ידי פולינום, ולכן גם הקוד הדואלי הוא ציקלי, והוא גם נוצר על ידי פולינום. מצא את הפולינום של $C^{\perp}$. (זהירות, הניסיון הראשון לא עובד, יש צורך בטוויסט!)

2.3 קודים בפולינומים רב־משתנים $(Reed-Muller\ Codes)$

זוהי הכללה של קודי ריד־סולומון.

הגדרה 2.14 יהיו $\mathbb{F} = \mathbb{F}_q$, $n = q^2$, $k = l^2$. נגדיר קוד מאורך n ומימד k באופן הבא:
במקום לחשוב על k־יה כוקטור, נחשוב עליה כריבוע של מספרים:

$$m = (m_{ij})_{i,j=0}^{l-1} = \sum_{i,j=0}^{n-1} m_{ij} x^i y^j$$

נעתיק את m ל־$\mathbb{F}^n$ ע"י הצבת כל הזוגות $(\alpha, \beta) \in \mathbb{F} \times \mathbb{F}$ בפולינום:

$$m(x,y) \to (m(\alpha,\beta))_{(\alpha,\beta)\in\mathbb{F}\times\mathbb{F}}$$

משפט 2.15 זהו $\left[q^2, l^2, \left(1 - \frac{2(l-1)}{q}\right) q^2\right]_q$־קוד.

הערה 2.16 נציין שוב כי המרחק בסימון מעלה מציין חסם תחתון.

ההוכחה תתקבל די מהר מהלמה הבאה:

למה 2.17 (The Schwartz-Zippel Lemma) בהנתן פולינום $Q(x_1, ..., x_m)$ מדרגה טוטלית[3] לכל היותר L, וקבוצה $S \subseteq \mathbb{F}$. אזי, הפולינום מתאפס על לכל היותר $\frac{L}{|S|} \cdot |S|^m$ מאיברי $\mathbb{F}^m \ni S^m$.

נוכיח תחילה את המשפט מתוך הלמה: **הוכחה:** ניישם ל־$S = \mathbb{F}_q$. אזי פולינום בשני משתנים ממעלה $L = 2(l-1) \geq \frac{L}{|S|} \cdot |S|^m = \left(\frac{2(l-1)}{q}\right) \cdot q^2$ מתאפס על לכל היותר $\left(\left(\frac{2(l-1)}{q}\right) - 1\right) \cdot q^2$ מאיברי $\mathbb{F}_q \times \mathbb{F}_q$, ולכן לא מתאפס על לפחות איברים, וזה נותן חסם תחתון על המרחק של הקוד. ■

ולסיום הדיון, נוכיח את הלמה: **הוכחה:** באינדוקציה על m.

[3] כלומר מסכמים את הדרגה של כל ה־x_i.

ל־$m=1$: הפולינום מתאפס על לכל היותר L איברים, וזה ידוע.
נניח באינדוקציה, ונכתוב:

$$Q\left(x_1,...,x_m\right)=\sum_{i=0}^{t}x_1^iQ_i\left(x_2,...,x_m\right)$$

כאשר t זו החזקה הגבוהה ביותר של x_1 המופיעה ב־Q, וברור $t\leq L$. כמו כן, דרגת Q_t $\geq L-t$. על פי הנחת האינדוקציה:

$$Q_t\left(x_2,...,x_m\right)\neq 0$$

עבור לפחות $\left(\frac{1-(L-t)}{|S|}\right)|S|^{m-1}$ מאיברי $S\times...\times S\subseteq S^{m-1}$.
נניח ש־$\left(s_1,...,s_m\right)\in S^{m-1}$ כך ש־$Q_t\left(s_2,...,s_m\right)\neq 0$, ונתבונן בפולינום $Q\left(x_1,s_2,...,s_m\right)$.
נותרנו אם כך עם פולינום ממעלה t במשתנה אחד, ולכן פולינום זה לא מתאפס על לפחות $|S|-t=\left(1-\frac{t}{|S|}\right)|S|$ איברים.
את הפעולה הזו אפשר לעשות עבור כל $(m-1)$־יה מתאימה, וכאמור יש לפחות $\left(\frac{1-(L-t)}{|S|}\right)|S|^{m-1}$ כאלו, ולכן בסה"כ Q אינו מתאפס על לפחות:

$$\left(1-\frac{L-t}{|S|}\right)|S|^{m-1}\cdot\left(1-\frac{t}{|S|}\right)|S|=|S|^m\left(1-\frac{L-t}{|S|}\right)\left(1-\frac{t}{|S|}\right)$$
$$=|S|^m\left(1-\frac{L}{|S|}+\frac{t\left(L-t\right)}{|S|^2}\right)\geq|S|^m\left(1-\frac{L}{|S|}\right)$$

■

לקודי ריד־מולר $(R-M)$ יש אינטרפטציות שונות - לרב משתמשים בו באופן הבא:
$\mathbb{F}=\mathbb{F}_q$, בחר $d\geq 1,\ m\geq d$. מקדדים מסר באורך $k=\begin{pmatrix}m+d\\m\end{pmatrix}$ = אוסף הפולינומים ב־m משתנים ממעלה $\leq d$ ע"י הערכת פולינום כזה בכל איבר $\mathbb{F}_q^m$, ומקבלים קוד ממימד $\begin{pmatrix}m+d\\m\end{pmatrix}$ באורך q^m.
תרגיל פשוט: חשב חסם תחתון על ה־$dist$.

לקודים אלו יש כל מיני שימושים חשובים. אם מגדילים את q ודואגים ליחס l/q קבוע, אז אלו קודים טובים, אבל ה־q כל הזמן גדל.

2.4 קודי BCH

13/11/2012

זוהי דוגמא חשובה לקוד ציקלי.
תזכורת: ראינו כי קוד ציקלי הינו תת מרחב של $\mathbb{F}_q^n$ האינווריאנטי תחת הזזה ימינה:

$$\left(a_1,...,a_n\right)\to\left(a_n,a_1,...,a_{n-1}\right)$$

כמו כן, ראינו כי קוד ציקלי שקול לאידאל בחוג:

$$R\left(x\right)=\mathbb{F}_q[x]/(x^n-1)$$

כמובן ומאחר ב־$\mathbb{F}_q[x]$ הוא חוג ראשי, אז קוד ציקלי נקבע לחלוטין ע"י הפולינום היוצר אותו, וזהו פולינום המחלק את x^n-1, כי אם $R \triangleright C = (g(x))$ אז $(x^n-1) \subseteq (g(x))$, ולכן $g(x) | x^n-1$.

טענה 2.18 $dimC = n - deg(g(x))$.

קוד BCH הינו קוד ציקלי, כאשר קובעים מראש חסם תחתון למרחק, ובונים בהתאם את הפולינום (קרי את הפולינום היוצר אותו).

נסמן: $\mathbb{E} = \mathbb{F}_{q^m}$, ובּ־$\mathbb{E}^*$ את החבורה הציקלית מסדר $n = q^m - 1$, כאשר w יוצר של $\mathbb{E}^*$.

עבור $\alpha \in \mathbb{E}^*$ נסמן $m_\alpha(x)$ את <u>הפולינום המינימלי של α מעל $\mathbb{F}_q$</u>. כזכור:

$$deg(m_\alpha(x)) = [\mathbb{F}_q(\alpha) : \mathbb{F}_q] \leq m$$

כמו כן, $m_\alpha(x) | x^n - 1$, כי הפולינום x^n-1 מאפס את כל איברי $\mathbb{E}^*$ (וביניהם α) שהסדר הכפלי שלהם הוא $n = q^m - 1$.

הערה 2.19 לכל $\alpha \in \mathbb{E}^*$, $m_{\alpha^q}(x) = m_\alpha(x)$, מאחר שהעתקת פרוביניוס $x \to x^q$ מקבעת את כל מקדמי m_α וכן מהווה אוטומורפיזם של $\mathbb{F}_{q^m}$, m_α מאפס גם את α^q, באותו האופן שבו m_{α^q} מאפס את α:

$$m_\alpha(\alpha^q) = (m_\alpha(\alpha))^q = 0$$

זה מראה ש־$m_{\alpha^q} | m_\alpha(x)$. הכיוון השני נובע מאי־פריקות של $m_\alpha(x)$, או מטיעון שקול על m_{α^q} ע"י הפעלת העתקת פרוביניוס $m-1$ פעמים (זהו אוטומורפיזם מסדר m ב־$Gal(\mathbb{F}_{q^m}/\mathbb{F}_q)$.

עובדה זו למעשה נובעת מהטענה הכללית הבאה:

טענה 2.20 תהי $\mathbb{E}/\mathbb{F}$ הרחבת גלואה, ותהי $G = Gal(\mathbb{E}/\mathbb{F})$. אזי, לכל $\sigma \in G$ מתקיים:

$$\forall \alpha \in \mathbb{E} \; m_{\sigma(x)}(x) = m_\alpha(x)$$

הגדרה 2.21 $BCH_q(m,r)$ הוא הקוד הנוצר כאידאל ע"י הפולינום:

$$h_r(x) := lcm\{ m_{w^i}(x) | \, 1 \leq i \leq r \}$$

הקוד תלוי בבחירת היותר w^i.

טענה 2.22 $BCH_q(m,r)$ הוא קוד $[n,k,d]_q$, כאשר:

$$n = q^m - 1, \;\; k \geq n - \frac{q-1}{q} \cdot m \cdot r, \;\; d \geq r+1$$

הוכחה: $k = n - deg\left(h\left(x\right)\right)$. תחילה, מאחר ש־$h$ הוא ה־lcm של r פולינומים, כל אחד מדרגה $m \geq$, הרי ש־$deg\left(h\left(x\right)\right) \leq m \cdot r$.

נשתמש בהערה האחרונה על מנת לשפר הערכה זו - מההערה, $m_{w^i} = m_{w^{q_i}}$, ולכן נוכל להתעלם מכל כפולה של q מבין $1 \leq i \leq r$. נקבל $\frac{q-1}{q} \cdot r$ פולינומים, קרי:

$$deg\left(h\right) \leq \frac{q-1}{q} \cdot m \cdot r$$

ולכן $k \geq n - \frac{q-1}{q} \cdot m \cdot r$.

לגבי המרחק - יש להוכיח כי אין מילת קוד עם משקל המינג $\geq r$. נניח בשלילה כי יש מילה שכזו:

$$b\left(x\right) = b_i x^{k_1} + ... + b_r x^{k_r}$$

כאשר $b_1, ..., b_r \in \mathbb{F}_q$ לא כולם 0, ו־$b\left(x\right) \in C$.

מכאן ש־$h_r\left(x\right) | b\left(x\right)$ בחוג R, כלומר קיימים $g_1\left(x\right), g_2\left(x\right) \in \mathbb{F}_q\left[x\right]$ עם:

$$b\left(x\right) = h_r\left(x\right) g_1\left(x\right) + g_2\left(x\right)\left(x^n - 1\right) \in \mathbb{F}_q\left[x\right]$$

אבל, אגף ימין מאפס את כל w^i, $1 \leq i \leq r$, שכן h_r מהגדרתו מאפס אותם, ו־$\left(x^n - 1\right)$ מאפס את כל $\mathbb{F}_{q^m}$. מכאן ש־$b\left(x\right)$ מאפס אותם גם הוא, קרי:

$$\begin{pmatrix} w^{k_1} & w^{k_2} & \cdots & w^{k_r} \\ w^{2k_1} & w^{2k_2} & \cdots & w^{2k_r} \\ \vdots & \vdots & \ddots & \vdots \\ w^{rk_1} & w^{rk_2} & \cdots & w^{rk_r} \end{pmatrix} \begin{pmatrix} b_1 \\ \vdots \\ \vdots \\ b_r \end{pmatrix} = 0$$

כאשר המטריצה הנ"ל הינה מטריצת ון־דר־מונדה של $w^{k_1}, w^{k_2}, ..., w^{k_r}$, ולכן הדטרמיננטה שלה היא:

$$\left(\prod_{i=1}^{r} w^{k_i}\right) \prod_{i<j} \left(w^{k_i} + w^{k_j}\right) \neq 0$$

כי הסדר הכפלי של w הוא $q^m - 1$, ולכן כל ה־w^{k_i}־אים שונים זה מזה. על כן, בהכרח $\begin{pmatrix} b_1 \\ \vdots \\ \vdots \\ b_r \end{pmatrix}$ הוא וקטור האפס, בסתירה. ■

הערה 2.23 נשים לב כי הטענה האחרונה איננה מבטיחה לנו קיום משפחה של קודי BCH טובים, זאת מאחר ואם $r > \varepsilon n$, אזי:

$$k = n - \frac{q-1}{q} \cdot log_{\varepsilon}\left(n\right) \cdot \varepsilon \cdot n \overset{n \to \infty}{\longrightarrow} -\infty$$

2.5 דיון ראשון - האם יש קודים ציקליים טובים?

זוהי שאלה פתוחה, בה נדון עוד בהמשך הקורס. פרופ' לובוצקי סבור, בניגוד לדעה הרווחת היום, כי אין קודים כאלו.

כעת כשאנחנו מכירים קודים ציקליים, נביט במספר משפטים הנוגעים לנושא, בתקווה לקבל אינטואיציה:

משפט 2.24 ($Berman,'67$) אם $\{C_n\}_{n\in I}$ משפחה של קודים ציקליים מאורך n מעל $\mathbb{F}_q$, $n\to infty$, כך ש:

1. $(q,n)=1$ לכל $n\in I$.
2. קיים קבוע l כך שלכל ראשוני $p|n$ לאיזה $n\in I$, $p\leq l$ (כלומר, ה-n-אים ב-I נוצרים מאוסף סופי של ראשוניים).

אזי, $\{C_n\}_{n\in I}$ <u>אינה</u> משפחת קודים טובה.

משפט 2.25 ($B-S-S,2005$) משפט $Berman$ נכון:

1. אם קיים $\varepsilon>0$ כך שלכל $p|n$ מתקיים $p\leq n^{\frac{1}{2}-\varepsilon}$.
2. לכל n, אם $\{C_n\}_{n\in I}$ גם $LDPC$.
3. נכון לכל n, אם $\{C_n\}_{n\in I}$ גם $locally\ testble$.

דוגמא לקוד שלא ידוע אם הוא טוב:

2.5.1 $Quadratic\ Residue\ Code$

יהיו p,l ראשוניים, p אי זוגי, ונניח ש-l שארית ריבועית מעל p - כלומר, יש פתרון למשוואה $x^2\equiv l\,(modp)$. כזכור, מחצית מאיברי $\mathbb{F}_q^*$ הם ריבועים, ומחצית אינם (כי $\mathbb{F}_p^*$ חבורה ציקלית מסדר זוגי). נסמן ב-Q את קבוצת הריבועים ב-$\mathbb{F}_q^*$, אזי $|Q|=\frac{p-1}{2}$.

הרעיון הוא שהקבוצה Q "מתפלגת באופן רנדומי" ב-$\mathbb{F}_p^*$ (כאשר $p\to\infty$), כלומר קשה לקבוע מתי איבר הוא ב-Q.

טענה 2.26 תהא $\mathbb{E}/\mathbb{F}_l$ הרחבה סופית שבה שורש יחידה p-אי, נסמנו ב-w. נתבונן ב:

$$\mathbb{E}[x]\ni f(x)=\prod_{j\in Q}\left(x-w^j\right)$$

אזי:

1. $f(x)\in\mathbb{F}_l[x]$.
2. $f(x)\,|x^p-1$.

הוכחה: :

1. נתבונן באוטומורפיזם פרוביניוס $a \to a^l$. אזי, לכל $Q \ni j \equiv b^2 \,(modp)$ מתקיים:
$w^j \to w^{jl}$, כאשר $jl \equiv (bx)^2 \,(modp)$.
מכאן ש־f מקובע תחת אוטומורפיזם זה, לכן $f \in \mathbb{F}_l[x]$.

2. מאחר ו־w מסדר p, הרי שכל חזקות w מסדר p, ולכן כל שורשי f הם מסדר p, דהיינו $f|x^p - 1$.

■

הגדרה 2.27 קוד השארית הריבועית מוד p הוא האידאל הנוצר ע"י $f(x)$ הנ"ל.

משפט 2.28 אם הקוד הנ"ל הוא קוד $[p,k,d]_l$, אזי $d \geq \sqrt{p}$, ו־$k = p - \left(\frac{p-1}{2}\right) = \left(\frac{p+1}{2}\right)$.

2.6 עקרון אי הוודאות

20/11/2012

לטרנספורם פוריה יש הכללה אבסטרקטית. באופן כללי, עקרון אי הוודאות אומר שעבור פונקציה מסויימת, או לפונקציה או לטרנספורם פוריה שלה יש תומך גדול.

הגדרה 2.29 תומך של פונקציה $f : G \to \mathbb{C}$ הינו הקבוצה:

$$supp(f) = \{\, g \in G |\, f(g) \neq 0\}$$

נציג את העיקרון בחבורות אבליות סופיות. זוהי תורה מאוד חשובה בקומבינטוריקה. נראה כיצד היא מתקשרת לקודים בהמשך.

2.6.1 חבורות אבליות סופיות

תהא G חבורה אבלית סופית, ותהא $f : G \to \mathbb{C}$ על f. ניתן לחשוב על f כאיבר בחוג חבורה:

$$\mathbb{F}[G] = \left\{ \sum_{g \in G} a_g \cdot g \,\middle|\, g \in G,\ a_g \in F \right\}$$

כאשר הכפל מוגדר כך שהתכונות החשובות נשמרות. אזי, אפשר לחשוב על f באופן הבא:

$$f \sim \sum f(g) \cdot g,\ g \in G$$

נשים לב כי החבורה לא צריכה להיות אבלית בשביל זה.
אם ניקח $G = \left\{1, x, ..., x^{n-1}\right\} \sim C_n \cong \mathbb{Z}/n\mathbb{Z}$, אזי:

$$\mathbb{F}[G] = \left\{ \sum_{i=0}^{n-1} a_i x^i \,\middle|\, g \in G,\ a_g \in F \right\} \simeq \mathbb{F}[x]/(x^n - 1)$$

נגדיר קונבולוציה על שני איברי G באופן הבא:

$$(f_1 * f_2)(g) = \sum_{x \in G} f_1\left(gx^{-1}\right) \cdot f_2(x)$$

הגדרה 2.30 קרקטר על חבורה אבלית G יסומן ב־χ, והוא הומומורפיזם:

$$\chi : G \to S^1 = \{ z \in \mathbb{C} | \, |z| = 1 \}$$

אוסף הקרקטרים על חבורה אבלית G מהווה חבורה ביחס לכפל:

$$(\chi_1 \cdot \chi_2)(g) = \chi_1(g) \cdot \chi_2(g)$$

נסמן חבורה זו ב־$\hat{G}$.

הגדרה 2.31 תהי $f : G \to \mathbb{C}$, ונתאים לה פונקציה $\hat{f} : \hat{G} \to \mathbb{C}$ המוגדרת באופן הבא:

$$\hat{f}(\chi) = \frac{1}{|G|} \cdot \sum_{g \in G} f(g) \cdot \overline{\chi(g)}$$

עקרון אי הוודאות ־ נוסח ראשון

משפט 2.32 תהי G חבורה אבלית סופית. אזי לכל $0 \neq f : G \to \mathbb{C}$:

$$|supp(f)| \cdot \left| supp\left(\hat{f}\right) \right| \geq |G|$$

כלומר, לא יכול להיות ששני התומכים הם "קטנים מידי".

עקרון אי הוודאות של אייזנברג הוא מקרה אחר של מצב שכזה.

"תזכורת" ־ תורת ההצגות
אם G חבורה סופית כלשהיא ו־$\mathbb{F}$ שדה, אם $\mathbb{F}[G]$ אלגברה פשוטה למחצה (זה מתרחש כאשר $char(\mathbb{F}) \nmid |G|$, ובפרט נכון תמיד אם $char(\mathbb{F}) = 0$), אזי:

$$\mathbb{F}[G] = \oplus_{i=1}^{r} M_{n_i}(D_i)$$

כאשר M_{n_i} הינו חוג המטריצות $n_i \times n_i$, ו־D_i היא אלגברה עם חילוק (כלומר, שדה לא קומוטטיבי) מעל שדה הרחבה של $\mathbb{F}$, ממימד סופי מעל $\mathbb{F}$.
אם $\mathbb{F} = \mathbb{C}$, אזי אין ל־$\mathbb{F}$ הרחבות סופיות. יתר על כן (משפט שיש להוכיח), מאחר ו־$\mathbb{C}$ סגור אלגברית, אין אלגברה עם חילוק מעליו, ולכן:

$$\mathbb{C}[G] = \oplus_{i=1}^{r} M_{n_i}(\mathbb{C})$$

אם בנוסף לכך G אבלית, אז $n_i = 1$ לכל i (אחרת היה קומוטטיבי), ואז:

$$\mathbb{C}[G] \simeq \mathbb{C}^{|G|}$$

לכאורה צד שמאל מעל המרוכבים, ולכן גם צד ימין, ואז האיזומורפיזם כמרחבים וקטוריים הינו טריוואלי. עם זאת, האיזומורפיזם כחוגים איננו טריוויאלי.
טרנספורם פוריה הינו האיזומורפיזם המפורש. המעבר מצד שמאל לצד ימין נתון כתרגיל (שאלה 3 בתרגיל 3).

נחזור לדוגמא:

$$\mathbb{C}[C_n] = {}^{\mathbb{C}[x]}/_{(x^n-1)}$$

השדה סגור אלגברית, ולכן ניתן לחלק את (x^n-1): נסמן את שורשי היחידה של n ב־$\xi \in \Phi_n$, אזי ניתן לרשום:

$$x^n - 1 = \prod (x - \xi)$$

נזכור כי משפט השאריות הסיני מהקורס מבנים אלגבריים 2 אומר כי:

$$\mathbb{C}[C_n] \simeq {}^{\mathbb{C}[x]}/_{(x^n-\xi)} \simeq \oplus_{\xi\in\Phi_n} {}^{\mathbb{C}[x]}/_{(x-\xi)} \simeq \mathbb{C}^n$$

מסקנה 2.33 תהי $f : G \to \mathbb{C}$, G חבורה אבלית סופית. אזי:

$$\left|supp\left(\hat{f}\right)\right| = dim\,\langle f\rangle$$

כאשר $\langle f\rangle$ הוא האידאל הנוצר ע"י f ב־$\mathbb{C}[G]$.

מדוע?

$$\mathbb{C}[G] \ni f \sim \hat{f} \in \mathbb{C}^{|G|}$$

שכן טרנספורם פוריה בצד ימין הוא איזומורפיזם בין הצדדים.
את החוג $\mathbb{C}^{|G|}$ קל להבין ־ מכפלה של שדות. ניקח ממנו איבר. מהו האידאל הנוצר ממנו ב־$\mathbb{C}^{|G|}$? בכל קואורדינטה שאיננה 0, אפשר לכפול בכל איבר ולהגיע לכל מקום, ואת השאר לכפול באפס. לכן, כל קואורדינטה שאיננה 0 תתקבל במלואה, ואת 0 לא נוכל "להציל מאפסיותו", ולכן האידאל המתקבל הוא "פירוש" של התומך של $\hat{f}$.
בתרגיל בית נשלים הפרטים בהוכחה זו.

מכאן נגיע לניסוח שני של עקרון אי הוודאות. צורה זו הרבה יותר פשוטה, שכן אין צורך בטרנספורם פוריה:

עקרון אי הוודאות ־ מעל למרוכבים

משפט 2.34 תהי G חבורה אבלית סופית. אזי, לכל $0 \neq f \in \mathbb{C}[G]$ מתקיים:

$$|supp\,(f)| \cdot dim\,\langle f\rangle \geq |G|$$

הערה 2.35 פה רואים את הקשר לקודים ־ $|supp\,(f)|$ הוא מרחק הקוד, ו־$dim\,\langle f\rangle$ הוא המימד, $|G| = n$.

נוכיח את העקרון בנוסח זה: **הוכחה:** נוכיח לכל G (כולל לא קומוטטיבית) ולכל F - נשים לב כי לנוסח הראשון לא היתה משמעות לחבורה לא אבלית.
יהי $f = \sum_{g \in G} a_g \cdot g \in F[G]$. נסמן:

$$D = \{ g \in G | \, a_g \neq 0 \} = supp(f), \ \langle f \rangle = span \{ h \cdot f | \, h \in G \}$$

אם $dim \langle f \rangle = t$, אזי קיימים $h_1, ..., h_t$ כך ש-$h_1 \cdot f, ..., h_t \cdot f$ הם בסיס לאידאל הנוצר ע"י f.
מהו התומך של $h \cdot f$?

$$supp(h \cdot f) = h\left(\sum a_g \cdot g \right) = \sum a_g \cdot h(g) = h \cdot D$$

נסמן $supp \langle f \rangle = \bigcup_{f' \in \langle f \rangle} supp(f')$. אזי:

$$|G| = |supp \langle f \rangle| = \left| \bigcup_{i=1}^{t} h_i \cdot D \right| \leq t \cdot |D| \overset{def}{=} dim \langle f \rangle \cdot |supp(f)|$$

כאשר בצד שמאל יש שיוויון של ממש במקום $\leq$ כי $f \neq 0$, ולכן אפשר ע"י הכפלה להזיז אותו לכל מקום שאינו אפס באידאל. ■

כעת - משפט שאינו טריוויאלי:

עקרון אי הוודאות החזק לחבורות ציקליות

משפט 2.36 אם $G = C_p$ חבורה ציקלית מסדר ראשוני p, ו-$0 \neq f : G \to \mathbb{C}$, אזי:

$$\overbrace{|supp(f)|}^{=wt(f)} + \overbrace{\left| supp\left(\hat{f} \right) \right|}^{=dim \langle f \rangle} \geq p + 1$$

זהו משפט שיהיה משמעותי בתורת הקודים.
הסבר למשפט:
נסמן $G = \left\{ 1, x, x^2, ..., x^{p-1} \right\}$. אז אפשר לראות את $0 \neq f : G \to \mathbb{C}$ כפולינום:

$$f(x) = \sum_{i=0}^{p-1} a_i x^i, \ deg(f(x)) < p$$

אזי:

$$supp(f) = \{ i | \, a_i \neq 0 \}$$

$\hat{f} : \hat{G} \to \mathbb{C}$ כאמור מוגדרת כך:

$$\hat{f}(\chi) = \frac{1}{|G|} \cdot \sum_{g \in G} f(g) \cdot \overline{\chi(g)}, \ \chi : G \to S^1$$

במקרה שלנו, כלומר כאשר $G=C_p$, χ נקבע לחלוטין ע"י תמונת היוצר של G, והוא חייב לעבור לאיזשהוא $\xi \in \Phi_p = \{ z \in \mathbb{C} | \, z^p = 1 \}$. על כן, נסמן $\chi = \chi_\xi$. אזי:

$$\hat{f}(\chi_\xi) = \frac{1}{p} \cdot \sum_i a_i \cdot \overline{\xi^i} = \frac{1}{p} \cdot f\left(\overline{\xi}\right)$$
$$\Rightarrow supp\left(\hat{f}\right) = \left\{ \chi_\xi | \, f\left(\overline{\xi}\right) \neq 0 \right\}$$
$$\Rightarrow \left| supp\left(\hat{f}\right) \right| = \left| \{ \xi \in \Phi_p | \, f(\xi) \neq 0 \} \right|$$

לכן, $\left| supp\left(\hat{f}\right) \right|$ הוא מספר שורשי היחידה מוד p ש־f לא מתאפסת עליהם, ומספר זה שווה ל־p פחות מספר שורשי היחידה ש־f כן מתאפסת עליהם. מספר זה שווה ל:

$$p - deg\left(gcd\left(f(x), x^p - 1\right)\right)$$

שכן דרגת ה־gcd הנ"ל היא מספר שורשי f שהם שורשי יחידה מוד p. לכן נוסח זה שקול לנוסח הבא:

2.6.2 עקרון אי הוודאות עבור פולינום ב־$\mathbb{C}[x]$

עקרון אי הוודאות החזק - נוסח ב'

משפט 2.37 לכל פולינום $0 \neq f(x) \in \mathbb{C}[x]$ ממעלה $p >$ מתקיים:

$$\overbrace{\#\{\xi \in \Phi_p | \, f(\xi) = 0\}}^{=: Z_p(f)} \leq |supp(f)| - 1 = wt(f) - 1$$

וכמו כן מתוך ההסבר, שקול לנוסח נוסף:

עקרון אי הוודאות החזק - נוסח ג'

משפט 2.38 לכל פולינום $0 \neq f(x) \in \mathbb{C}[x]$ ממעלה $p >$ מתקיים:

$$(deg\left(gcd\left(f(x), x^p - 1\right)\right) =) \leq |supp(f)| - 1 = wt(f) - 1$$

זהו חסם הדוק - נראה זאת בעזרת דוגמאות.

דוגמאות:

1. $f(x) = x - 1$. מספר שורשים: 1, $wt(f) = 2$.
2. מקרה בו העקרון לא מתקיים:

$$f(x) = x^p - 1 \Rightarrow wt(f(x)) = 2, \; Z_p(f) = p \Rightarrow p \not\leq 2 - 1$$

אבל זהו פולינום ממעלה p, כלומר אין זו סתירה לעקרון, אלא דוגמא לעדינות של החסם.

3.

$$f(x) = 1 + x + ... + x^{p-1} = \frac{x^p - 1}{x - 1} \Rightarrow wt(f) = p,\ Z_p(f) = p - 1$$
$$\Rightarrow p - 1 \leq p - 1$$

4. אם התומך של f מרוכז בחזקות הנמוכות, אז $wt(f) - 1 = deg(f)$, והמשפט כבר מוכר היטב.

בפעם הבאה נוכיח את המשפט.

כעת, נשאל מדוע המשפט רלוונטי לתורת הקודים? ישירות ממנו נקבל שיש קודים טובים ציקליים, אבל <u>מעל המרוכבים</u>. אבל, זה לא מסובך מידי - למעשה, גם $R - S$ נותן את התוצאה הזו.

איך מקבלים מהעקרון (באופן אבסטרקטי) את הקודים האלו?

טענה 2.39 יש קודים ציקליים טובים מעל $\mathbb{C}$.

הוכחה: נסמן את קבוצת הראשוניים האי זוגיים ב־P. כאמור, קוד ציקלי מאורך n הוא אידאל בתוך $R = {}^{F[x]}/_{(x^n-1)}$.

קוד ציקלי טוב פירושו אידאל שמימדו לינארי ב־n, ומרחקו גם כן לינארי ב־n. לכל $p \in P$:

$$R = {}^{\mathbb{C}[x]}/_{(x^p-1)} \cong \mathbb{C}^p$$

נבחר אידאל I ממימד $\frac{p-1}{2}$ ב־$\mathbb{C}^p$. הוא קוד ציקלי כי הוא אידאל, ומימדו לינארי ב־n. נותר אם כך רק לבדוק את המרחק:

אם $0 \neq f \in I$ פולינום מדרגה $< p$, מהעקרון מתקיים:

$$|supp(f)| + dim\langle f \rangle \geq p + 1$$

אבל $dim\langle f \rangle \leq \frac{p-1}{2}$, ולכן $|supp(f)| \geq \frac{p+1}{2}$, ועל כן גם המרחק לינארי ב־$n = p$, כנדרש. ■

27/11/2012

נוכיח את הניסוח השני של עקרון אי הוודאות בעזרת טריק נחמד. נשים לב כי לניסוח השלישי יש משמעות מעל כל שדה $\mathbb{F}$.

אזהרה: הוא לא נכון בהכרח מעל כל שדה, אבל קל לנסחו.

נוכיח משפט עזר:

עקרון אי הוודאות - נוסח מעל שדה עם קרק' p

משפט 2.40 יהי F שדה עבורו $char(F) = p$, ויהי $0 \neq f(x) \in F[x]$ ממעלה $< p$. אזי:

$$deg(gcd(f(x), x^p - 1)) \leq wt(f(x)) - 1$$

הוכחה: בקרק' p, $x^p-1=(x-1)^p$, ולכן משמעות משפט זה היא שהריבוי של 1 כשורש של $f(x)$ חסום ע"י $wt(f(x))-1$.

נוכיח את המשפט באינדוקציה על $deg(f(x))$:

בסיס: אם $deg(f(x))=0$, אז $f(x)=c$ עבור $c\neq 0$. 1 איננו שורש של הפולינום, ולכן הריבוי הוא 0, וכמו כן

$$wt(f(x))-1=1-1=0\leq 0$$

כלומר הטענה נכונה.

צעד: נניח שהוכחנו עבור פולינום מדרגה $m>$, ונוכיחו לפולינום מדרגה m. נסמן $f(x)=\sum_{i=0}^{m}a_ix^i$, כאשר $a_m\neq 0$. נתבונן ב־a_0:

אם $a_0=0$, נחליף את $f(x)$ ב־$g(x)=\frac{f(x)}{x}$. נשים לב כי $wt(g(x))=wt(f(x))$, וכן $gcd(f(x),(x-1)^p)=gcd(g(x),(x-1)^p)$, ועל כן אין בעיה עם החלפה זו. כמו כן, $g(x)$ הוא פולינום מדרגה $m-1$, ולכן מהנחת האינדוקציה הטענה נכונה.

אחרת, כלומר אם $a_0\neq 0$, נתבונן בנגזרת של הפולינום:

$$f'(x)=a_1+2a_2x+...+ma_mx^{m-1}$$

מתקיים:

$$deg(f'(x))<deg(f(x)),\ wt(f'(x))\leq wt(f(x))-1$$

נשים לב כי אם $f(x)=(x-1)^a\cdot h(x)$ לאיזה $0\neq a\in\mathbb{N}$ כאשר $h(1)\neq 0$, ז"א $(x-1)\nmid h(x)$. אזי:

$$\begin{aligned}&f'(x)=a(x-1)^{a-1}h(x)+(x-1)^a\cdot h'(x)\\&\Rightarrow deg(gcd(f'(x),(x-1)^p))=a-1\end{aligned}$$

מדוע? ברור כי הדרגה היא לפחות $a-1$. היא לא a, כי אז $f'(x)$ היה מתחלק ב־$(x-1)^a$ - אבל בעוד שחלקו הימני מתחלק, השמאלי לא. כמו כן $f(x)$ לא מתחלק בו, כי:

$$\begin{aligned}&g(x):=\frac{f(x)}{(x-1)^{a-1}}=a\cdot h(x)+(x-1)\cdot h'(x)\\&\Rightarrow g(1)=a\cdot h(1)\neq 0\end{aligned}$$

לכן נוכל להפעיל את הנחת האינדוקציה על הפולינום $f'(x)$, ונקבל:

$$\begin{aligned}&a-1\leq wt(f'(x))-1=wt(f(x))-2\\&\Rightarrow a\leq wt(f(x))-1\end{aligned}$$

כנדרש. ■

כיצד נהפוך נשתמש בהוכחה זו ע"מ להוכיח את עקרון אי הוודאות בנוסח השני? נעשה שימוש בטכניקה של אלגברה קמוטטיבית בשם $Specialization$, הנובעת ממשפט האפסים של הילברט:

הגדרה 2.41 שדה מספרים K הוא שדה המהווה הרחבה סופית של $\mathbb{Q}$ (ובפרט הסגורים האלגבריים מקיימים $\tilde{K}=\tilde{\mathbb{Q}}$).

למשל: $K=\mathbb{Q}\left(\sqrt{2}\right)\ ,\ K=\mathbb{Q}\sqrt[p]{1}$.

משפט 2.42 יהי K שדה מספרים, ויהיו $a_1,..,a_n\in\mathbb{C}$. נסמן את החוג $R=K\left[a_1,...,a_n\right]$ (אין סיפוח של ההפכי), ויהי $0\neq\alpha\in R$.
אזי, קיים הומומורפיזם של חוגים $\varphi:R\to\tilde{K}$ כך ש:

$$\varphi\left(\alpha\right)\neq0,\ \varphi_K=id$$

לא נוכיח משפט זה מסגרת הקורס, אך נשתמש בו: **הוכחה:** תחילה, נראה כי ניתן מספיק להוכיח את המשפט עבור פולינום שמקדמיו אלגבריים:
נסמן $f\left(x\right)=\sum_{i=0}^{p-1}a_ix^i\ ,\ a_i\in\mathbb{C}$. נסמן:

$$\alpha=\prod\left\{a_i\middle|\,a_i\neq0\right\}$$

ונסמן $K=\mathbb{Q}\left(\sqrt[p]{1}\right)=\mathbb{Q}\left(e^{\frac{2\pi i}{p}}\right)$, $R=K\left[a_1,...,a_n\right]$. אזי, מהמשפט מעלה, קיים הומו' $\varphi:R\to\tilde{K}=\tilde{\mathbb{Q}}$ כך ש:

$$\varphi\left(\alpha\right)\neq0,\ \varphi|_K=id$$

נסמן:

$$\overline{f}\left(x\right)=\varphi\left(f\left(x\right)\right)=\sum_{i=0}^{p-1}\varphi\left(a_i\right)\cdot x^i$$

נשים לב כי:

1. $wt\left(\overline{f}\left(x\right)\right)=wt\left(f\left(x\right)\right)$, כי $\varphi\left(\alpha\right)\neq0$, ולכן לכל $a_i\neq0$, $\varphi\left(a_i\right)\neq0$.
2. אם $\xi\in\Phi_p$ שורש של $f\left(x\right)$, אזי ξ גם שורש של $\overline{f}\left(x\right)$, כי K משרה את הזהות על φ.

לכן, מספיק להוכיח את המשפט עבור $\overline{f}\left(x\right)$, שהוא פולינום שמקדמיו אלגבריים.
שנית, נבצע רדוקציה נוספת של הבעיה לקרק' p, ורדוקציה זו תסיים את הוכחת המשפט, שכן נכונות העקרון לרדוקציה היא בדיוק משפט העזר אותו הוכחנו. לשם כך, נזדקק למידע נוסף מקורסים מתקדמים:

כאמור $R = K[a_1, .., a_n]$, ו־K הרחבה סופית של $\mathbb{Q}$. נסמן ב־$\mathcal{O}$ את חוג השלמים האלגבריים של K:

$$\mathcal{O} = \left\{ \alpha \in K \,\middle|\, \exists b_0, ..., b_{l-1} \in \mathbb{Z},\ s.t.\ \alpha^l + \sum_{i=0}^{l-1} b_i \alpha^i = 0 \right\}$$

כלומר שורשי פולינומים מתוקנים מעל $\mathbb{Z}$, למשל:

1. אם $K = \mathbb{Q}(\sqrt{2})$, אזי $\mathcal{O} = \mathbb{Z} + \mathbb{Z}[\sqrt{2}]$ (שלם אלגברי רציונלי הוא שלם ממש - b_i חייבים להיות ± 1).
2. אם $K = \mathbb{Q}(i)$, אזי $\mathcal{O} = \mathbb{Z}[i]$.

כמה עובדות על $\mathcal{O}$:

- $\mathcal{O} \subseteq K,\ \mathbb{Z} \subset \mathbb{Q}$, ונסמן $d = dim_{\mathbb{Q}} K$. אזי $\mathcal{O} \simeq \mathbb{Z}^d$ כחבורה.
- לכל אידאל ראשוני (ובמקרים אלה - מקסימלי) (p) ב־$\mathbb{Z}$, קיים אידאל ראשוני מאינדקס סופי $\pi \lhd \mathcal{O}$ כך ש־$\pi \cap \mathbb{Z} = (p)$.

  מכך קל לראות ש:

$$\mathbb{F}_p = \mathbb{Z}/\mathbb{Q} \subseteq \mathcal{O}/\pi$$

  שדה סופי. נסמנו ב־F. אזי נקבל שיכון לתוך שדה סופי $\mathbb{Z} \to \mathcal{O} \to \mathcal{O}/\pi$.

- כל איברי $\alpha \in K$ ניתנים לכתיבה כ־$\alpha = \frac{r}{s}$ כאשר $r, s \in \mathcal{O}$. מכאן נובע כי לכל $\alpha \in K$ קיים $s \in \mathcal{O}$ כך ש־$s \cdot \alpha \in \mathcal{O}$.

  נחזור ל־$f(x) \in K[x]$. מהניתוח מעלה, ניתן לכפול אותו בסקלר מהשדה t כך ש:

$$\tilde{f}(x) = t \cdot f(x) \in \mathcal{O}[x],\ 0 \neq \tilde{f}(x)\,(mod\pi) \in F[x]$$

  נסמן $\eta : \mathcal{O} \to \mathcal{O}/\pi = F$, ויהי $\tilde{\tilde{f}}(x) = \eta\left(\tilde{f}(x)\right)$. אזי $wt\left(\tilde{\tilde{f}}(x)\right) \leq wt(f(x))$, כי אם $\xi \in \Phi_p$, אזי:

  1. $\xi \in \mathcal{O}$, כי $x^p - 1$ מאפס אותו.
  2. $\eta(\xi) = 1$, כי $\xi^p = 1$, ולכן $\eta(\xi)^p = 1 \in F \Leftrightarrow (\eta(\xi) - 1)^p = 0$.

  אבל F הוא שדה סופי מקרק' p, ולכן אם ξ שורש של $f(x)$, הוא גם שורש של $\tilde{f}(x) = t \cdot f(x)$ ותמונתו 1, ולכן שורש של $\tilde{\tilde{f}}(x)$.

  כעת:

$$gcd(f(x), x^p - 1) = gcd(t \cdot f(x), x^p - 1)$$

והמעלה לא תרד (מי שמחלק הוא פולינום מתוקן, לכן ישאר מאותה המעלה). הריבוי של 1 כשורש של $\tilde{\tilde{f}}(x)$ $\leq \#\{\xi \in \Phi_p \,|\, f(\xi) = 0\}$, ואם נציב גם את אי השיוויון שכרגע הוכחנו ואת משפט העזר מתחילת השיעור, נקבל:

$$\{\xi \in \Phi_p \,|\, f(\xi) = 0\} \leq wt\left(\tilde{\tilde{f}}(x)\right) - 1 \leq wt(f) - 1$$

כנדרש! ■

2.6.3 עקרון אי הוודאות בשדות סופיים, והקשר לקודים ציקליים טובים

בפעם הקודמת הוכחנו את עקרון אי הוודאות החזק. ראינו 3 נוסחים אקוויולנטיים. כמו כן, בשיעור שלפניו גם הראנו בעזרת העקרון כי יש קודים ציקליים טובים מעל המרוכבים.

היום נדבר על מה כֵן קורה בשדות סופיים: לעיתים העקרון אינו נכון, ולעיתים העיקרון נכון אך לא עוזר במציאת קודים ציקליים טובים.

טענה 2.43 יהא l ראשוני, $F=\mathbb{F}_l$, l קבוע, ויהי p ראשוני כך ש־$p\neq l$, ונביט ב־$R=_{F[x]/(x^p-1)}$. נסמן את הסדר של l כאיבר בחבורה הכפלית $\mathbb{F}_p^*$ להיות $r=ord_p(l):=min\left\{i>0|\, l^i\equiv 1\,(modp)\right\}$. אזי:

$$R\simeq \mathbb{F}_l\times\left(\mathbb{F}_{l^r}\right)^{\frac{p-1}{r}=s}$$

כאיזומורפיזם של חוגים.

הערה 2.44 נשים לב כי $r|p-1$, כי l הוא איבר מסדר r בחבורה מספר $p-1$ (ממשפט לגראנג').

הערה 2.45 תוצאה זו איננה מפתיעה, שכן:

$$x^p-1\overbrace{=}^{\in\mathbb{F}_l[x]}g_0(x)\cdot g_1(x)\cdot\ldots\cdot g_s(x)$$

כאשר g_i פולינומים אי פריקים שונים מספרביליות - אם אחד מהפולינומים היה מופיע יותר מפעם אחת, אזי ל־(x^p-1) היה שורש כפול, ואז נגזרתו היתה מחלקת אותו - בסתירה לכך שהיא זרה, מהגדרת הפולינום. על כן אין שורשים כפולים, וע"י שימוש בורסיה של משפט השאריות הסיני, נקבל:

$$\mathbb{F}_l[x]/_{(x^p-1)}\simeq\prod_{i=0}^{s}\mathbb{F}_l[x]/_{g_i(x)}$$

ולכן מצד ימין אנו מקבלים אידאלים מקסימליים. אנחנו בהוכחה שלנו נזהה את השדות המתקבלים. אם אחד הגורמים הוא מסדר 1 $(g_0=x-1)$, הוא נותן פולינום ממעלה 1, והמנה היא פשוט השדה $\mathbb{F}_l$. על כן, מטרתנו היא להוכיח כי יש גורם יחיד מסדר 1, והשאר גורמים מסדר r (למרות היותם פולינומים שונים זה מזה).

הוכחה: נשתמש בסימון g_i מההערה מעלה, ונראה כאמור כי ישנו גורם אחד g_0 ממעלה 1 במכפלה, והשאר כולם ממעלה r.

מאחר ו־$l^r\equiv 1\,(modp)$, ז"א $p|l^r-1$, ולכן השדה $\mathbb{F}_{l^r}$ מכיל שורש p של היחידה ($\neq 1$), כי $\mathbb{F}_{l^r}^*$ היא חבורה ציקלית מסדר l^r-1. אולם, אם השדה מכיל שורש p של היחידה, הוא מכיל גם את שאר שורשי p של היחידה (כי p ראשוני), ולכן לכל שורש יחידה ξ מסדר p ב־$\mathbb{F}_l$, מעלת הפולינום המינימלי המאפס אותו $r\geq$ ממשפט מהקורס מבנים אלגברים :

$$deg(m_\xi)=[F[\xi]:F]$$

לכן $deg(g_i)\leq r$.

מצד שני, אם $deg(g_i(x))<1$ לאיזשהוא $i\neq 0$, אזי יש שורש יחידה η מסדר p ושדה $\mathbb{F}_{l^{r'}}$ כך ש־$\eta\in\mathbb{F}_{l^{r'}}$ (כי $deg(g_i(x))=r'=[\mathbb{F}_l[\eta]:\mathbb{F}_l]$). אבל, זה גורר כי $p|l^{r'}-1$ (שוב ממשפט לגראנג'), כלומר מצאנו $r'<r$ כך ש־$l^{r'}\equiv 1\,(modp)$, בסתירה להגדרת r.■

הערה 2.46 יכולנו גם להוכיח זאת בעזרת כפולי גלואה, כאשר השורשים המשותפים של g_i היו כפולים אלו, אבל בעזרת ההוכחה מעלה אנו רואים בדיוק מיהם האיברים, דבר שיעזור לנו בהמשך.

נשתמש בתוצאה זו כדי לבחון את עקרון אי הוודאות.

הגדרה 2.47 l יקרא פרימיטיבי מודולו p, אם l יוצר את $\mathbb{F}_p^l$, כלומר אמ"מ $ord_p(l) = p-1$.

טענה 2.48 אם l פרימיטיבי מודולו p, אזי עקרון אי הוודאות החזק מתקיים עבור p מעל $\mathbb{F}_l$.

הוכחה: נוכיח את קיום העקרון לפי הנוסח השני שלו.
אנו רוצים להראות כי:

$$\#\{\xi \in \Phi_p \,|\, f(\xi) = 0\} \leq wt(f) - 1$$

נשים לב כי המשמעות היא ש־$\frac{x^p-1}{p-1}$ הוא פולינום אי פריק ב־$\mathbb{F}_l[x]$ - כי יש s גורמים מאותה המעלה: $\frac{x^p-1}{p-1} = \prod_{i=1}^{s} g_i(x)$, ואם הדרגה כבר $p-1$, אז יש שם רק גורם אחד, כלומר הפולינום אי פריק. אם יש פולינום שמאפס איזשהוא שורש יחידה מסדר p, הוא חייב להיות ממעלה $p-1$ ומעלה, ולכן עקרון אי הוודאות מתקיים באופן טריוואלי.
אפשר גם להוכיח את העקרון לפי הניסוח שהבאנו לחבורות ציקליות:

$$wt(f(x)) + dim\langle f(x)\rangle \geq p+1$$

כאשר $0 \neq f \in \mathbb{C}[x]$, $deg(f) < p$, p ראשוני, $R = {}^{\mathbb{C}[x]}/_{(x^p-1)}$, ו־$\langle f(x)\rangle$ האידאל של R הנוצר ע"י $f(x)$.
מהמשפט הקודם:

$$R = \mathbb{F}_l \oplus \mathbb{F}_{l^{p-1}} = \overbrace{\mathbb{F}_l[x]/(x-1)}^{I} \oplus \overbrace{\mathbb{F}_l[x]/\left(x^{p-1}+x^{p-2}+\ldots+x+1\right)}^{II}$$

האידאלים בשדות האלה הם עצמם, 0, או הכל.
אם הפולינום ב־$\mathbb{F}_l$, מכיוון והפולינומים ב־I מתאפסים ב־II, המשקל שלו הוא p, מספר שורשיו הוא $p-1$, ונקבל:

$$wt(f(x)) + dim\langle f(x)\rangle \geq p+1$$

ולכן העקרון מתקיים.
אחרת הוא ב־$\mathbb{F}_{l^{p-1}}$, ואז השורש היחיד שלו ב־I, ומשקלו הוא 2, אך במקרה זה המימד של האידאל הנוצר גדול מספיק כדי לקיים את העקרון. ■

מכאן אנו מגיעים להשערת ארטין המפורסמת:

השערת ארטין בהנתן l קבוע, יש ∞ p־אים כך ש־l פרימיטיבי מודולו p.
(מאמינים שהיא נכונה כי היא נובעת מהשערת רימן).

זה טוב - אבל מאוד לא יעיל... מדוע?
ראינו שכל פולינום באידאל משקלו הוא לפחות $\frac{s}{2}$. כאן, מהם האידאלים? אין הרבה ממה לבחור:

- $\mathbb{F}_l$ - קטן מידי, צריך אחוז קבוע ב־F.
- $\mathbb{F}_{l^{p-1}}$ - מכיל כמעט את כל הפולינומים, וחסם על המשקל לא יעיל, לכן הקוד המתקבל לא טוב.

מה כן היינו רוצים\שמחים שיהיה? עוד מקרה מעניין -

הגדרה 2.49 מספר ראשוני p מהצורה $p=2^n+1$ נקרא ראשוני של פרמה.

אלו מעניינים בקונטקסט הזה, כי אם למשל נביט במקרה הכי מעניין $l=2$:

$$ord_p(2) \leq log_2(p+1),\ 2^n \equiv 1\,(modp) \Rightarrow n|p-1$$

אזי במקרה הזה, נקבל:

$$R = \mathbb{F}_l \oplus \left(\mathbb{F}_{2^n}\right)^{\frac{p-1}{n}}$$

2.6.4 מה צריך להוכיח בתורת המספרים כדי לקבל קודים ציקליים טובים?

יהי F שדה קבוע, p ראשוני. נסמן:

$$\mathcal{M}_F(p) = min\left\{wt(f(x)) + \#\left\{\xi \in \Phi_p \middle| f(\xi) \neq 0\right\} \middle| 0 \leq f(x) \in F[x],\ deg(f(x)) < p\right\}$$

כזכור, עקרון אי הוודאות החזק אומר:

1. $\mathcal{M}_{\mathbb{C}}(p) \geq p+1$.
2. $\mathcal{M}_{\mathbb{F}_l}(p) \geq p+1$ אם l פרימיטיבי מודולו p.
3. $\mathcal{M}_F(p) \geq p-1$ אם $char(F)=p$.

ראינו (בתרגילים) מקרים בהם $\mathcal{M}_F(p) < p+1$.

טענה 2.50 יהא l ראשוני, $F=\mathbb{F}_l$. נניח שקיים $\delta > 0$ וקבוצה אינסופית של ראשוניים P כך ש:

1. לכל $p \in P$, $\mathcal{M}_F(p) \geq \delta p$.
2. $ord_p(l) \leq (1-\delta)\,\delta p$.[4]

אזי יש אינסוף קודים ציקליים טובים מעל $\mathbb{F}_l$.

[4] תנאי זה יבטיח שנוכל למצוא אידאל, ממנו נוכל לבנות קוד ציקלי טוב

הוכחה: יהא $p \in P$, ונסמן $R = {F[x]}/{(x^p-1)}$. ראינו:

$$R = F \oplus (\mathbb{F}_{l^r})^s$$

כאשר $r = ord_p(l)$. נבחר ב־R אידאל I כך ש:

$$\frac{1-\delta}{2} \cdot \delta p \leq dim(I) \leq (1-\delta) \cdot \delta p$$

מדוע זה אפשרי?
זה שווה ערך לבחירה של סכום חלקי של שדות - מימד של אחד מהם הוא r, ומ־2 אנו יודעים כי $r \leq (1-\delta) \cdot \delta p$. אם הוא כבר $\leq \frac{1-\delta}{2} \cdot \delta p$, סיימנו. אחרת הוא קטן ממחצית $\delta p \cdot (1-\delta)$, ולכן הוספה של שדה נוסף ממימד r לא יעבור את החסם המבוקש. שוב נבדוק - אם האידאל עדיין לא מקיים $\leq \frac{1-\delta}{2} \cdot \delta p$, אז נוכל להוסיף עוד, וכך הלאה, עד לקבלת אידאל מתאים.

מימד הקוד גדל עם p ולכן לינארי. נותר להוכיח כי המשקל הוא טוב. ניקח $0 \neq f(x) \in I$. מקיום התכונה הראשונה:

$$wt(f(x)) + \#\{\xi \in \Phi_p | f(\xi) \neq 0\} \geq \delta p$$

כדי למצוא את $wt(f(x))$, עלינו לראות על כמה שורשי יחידה p־אים f כן\לא מתאפס?

$$R = \mathbb{F}_l \uplus_{i=1}^{s} {\mathbb{F}_l[x]}/{\xi_i(x)}$$

פולינום ב־I מתאפס על לפחות $coDim(I)$ בתוך R (הוא 0 בשאר השדות), כלומר השאר מחלקים אותו. כל אחד כזה מתאפס על הרבה שורשי יחידה, לכן מספר שורשי היחידה שהוא מאפס הוא הקו־מימד.

על כן פולינום שכזה אינו מתאפס על $\geq dim(I)$ שורשי יחידה, ולכן נקבל כי:

$$\begin{aligned} &wt(f(x)) + dim(I) \geq \delta p \\ &\Rightarrow wt(f(x)) \geq \delta p - dim(I) \geq \delta p - (1-\delta)\delta p = \delta^2 p \end{aligned}$$

ועל כן, גם המשקל גדל לינארית ב־p, ואכן קיבלנו קוד ציקלי טוב. מכיוון ויש אינסוף ראשוניים p כאלה, נקבל אינסוף קודים ציקליים טובים, כנדרש. ■

2.7 קודים דואליים לקודי BCH, קודי האדמר ואפליקציות

11/12/2012

נזכיר כי אם ${E}/{F}$ הרחבת שדות, כאשר

...

3 גרפים וקודים

18/12/2012

יהא $X = (V, E)$ גרף סופי קשיר כלשהוא. נסתכל על המרחב הנפרש ע"י הקשתות מעל $\mathbb{F}_2$ - נסמנו ב־$\mathbb{F}_2^E$, אשר איבריו הם תת קבוצות של קשתות. אפשר גם לחשוב על המרחב הזה באופן הבא:

$$\mathbb{F}_2^E = \{f | E \to \mathbb{F}_2\}$$

נגדיר בתוכו קוד C להיות המרחב הנפרש ע"י המעגלים הסגורים בגרף.
נחשב על הקוד הזה מבחינת הביצועים שלו בתורת הקודים - מה המרחק ומה ה-$rate$ שלו?
בדר"כ E הרבה יותר גדול מ-V, למשל בעץ.

הגדרה 3.1 $girth\left(X\right)$ מוגדר להיות אורך המעגל הסגור הקטן ביותר (בעברית - מותן).

אי שיוויון מור

טענה 3.2 אם X גרף k-רגולרי:

$$girth\left(X\right) \leq 2 \cdot log_{k-1}\left(|V|\right) = 2 \cdot log_{k-1}\left(\frac{2\left|E\right|}{k}\right) \cong 2\left(log\left(E\right) - 1\right)$$

לקודים כאלה קוראים $cycle\ code$. מהטענה שבשיעורי הבית, קיבלנו כי בעוד ה-$rate$ טוב, המרחק גדול מאוד, כלומר הקוד לא יעיל. עם זאת, הבניה הזו חשובה, ונראה זאת בהמשך.

3.1 מקודים לגרפים

קוד C הוא תת מרחב ממימד k של $\mathbb{F}_2^n$.
אפשר לחשוב על C כמרחב מערכת הפתרונות של מטריצה H (שנהוג לקרוא לה $parity\ check\ matrix$ - מטריצת בדיקת הזוגיות) מגודל $m \times n$ מעל $\mathbb{F}_2$, כך ש:

$$C = \left\{\alpha \in \mathbb{F}_2^n \,\middle|\, H\alpha = \vec{0} \in \mathbb{F}_2^m\right\},\ m \geq n - k$$

הערה 3.3 H לא נקבעת באופן יחיד ע"י C (תת המרחב יכול להיות תשובות למערכות משוואות שונות).

עד כה בקורס התעלמנו מהאלגוריתמיקה של $encoding$ ו-$decoding$. בעזרת מטריצה H אפשר לבדוק אם מילה בקוד, ולכן יש לה חשיבות רבה בספרות המעשית של תורת הקודים.
לכן רוצים לשמור על H כמטריצה "קלה" מבחינת מספר האחדות שיש בה.
נתאים ל-H גרף <u>דו צדדי</u> $X = \left(\overbrace{L}^{V}, R, E\right)$, כאשר $n = L$ הביטים, ו-m - R המשוואות המגדירות, ויש קשת בין ביט למשוואה אם הוא מופיע בה.
מילה היא בעצם השמה בצד שמאל. אם נרצה לבדוק אם מילה בקוד או לא, נסכום לכל קודקוד בצד ימין את השכנים שלו (בצד שמאל), ואם המילה בקוד, הסכום יהיה 0. באופן כללי: $H_{ij} \neq 0$ אומר שהביט ה-j מופיע במשוואה ה-i.

את הדוגמא הראשונה שראינו בתחילת השיעור ניתן להציג אותה באופן אלגנטי באופן הבא - $|E| = n,\ |V| = m$, ויש קשת בין קודקודים אם יש קשת ביניהם בגרף המקורי. קיבלנו אם כך גרף דו צדדי מהגרף המקורי - גרף זה נקרא "גרף הקשתות מול הקודקודים". מילה היא חוקית אם סכום הקשתות הנוגעות בכל V הוא 0. הגרפים האלו לפעמים רגולריים בשני הצדדים, ונראה זו בהמשך.

3.1.1 ניתוח תכונות הקוד

כדי שיהיה $rate$ טוב, רצוי ש־$m << n$ (או לפחות שיהיו הרבה תלויות). מה צריך כדי שבקוד כזה ה־$distance$ יהיה טוב?

לכל תת קבוצה $S \subseteq L$, נסמן ב־$\Gamma(S)$ את שכני S.

מרחק יהיה טוב לקוד המתקבל מהגרף (L, R, E) נרצה שקבוצה "קטנה" מספיק לא תהיה בקוד, כלומר שקיים $y \in R$ שנוגע בבדיוק במספר אי זוגי של S. נסמן:

$$\Gamma_{odd}(S) = \{y \in \Gamma(S) \,|\, y \text{ "touches" } S \text{odd number of times}\}$$

איך משיגים את זה?
נסמן:

$$\Gamma_{unique}(S) = \{y \in R \,|\, y \text{ "touches" } S \text{exactly once}\}$$

ברור כי:

$$\Gamma_{unique}(S) \subseteq \Gamma_{odd}(S)$$

מסקנה 3.4 אם קוד C ניתן ע"י גרף דו צדדי (L, R, E) כמקודם: $|L| = n \;\; |R| = m$ ואם לכל $\phi \neq S \subseteq L$ מגודל $\delta n >$, $\Gamma_{odd}(S) \neq \phi$ מתקיים, אזי:

$$distance(C) \geq \delta n \Rightarrow \frac{dist}{n} \geq \delta$$

כאן קיבלנו קישור בין תכונה גרפית לבין תכונה של הקוד.

כאן אנחנו מגיעים למאמר מ־98 שעשה שימוש גרפים מרחיבים ־ אקספנדרים[5]:

הגדרה 3.5 גרף דו צדדי $X = (L, R, E)$, $|L| = n, \;\; |R| = m$ יקרא (γ, δ)־אקספנדר, אם לכל $S \subseteq L$ מגודל $\delta n >$, $|\Gamma(S)| \geq \gamma |S|$.

הרעיון: γ, δ יהיו גבוהים, בעוד $n, m \to \infty$.

הגדרה 3.6 גרף דו צדדי יקרא c־רגולרי, אם צד שמאל הוא c־רגולרי.

משפט 3.7 לכל $\varepsilon > 0$, אם c מספיק גדול, אזי כאשר $n \to \infty$, יש גרף דו צדדי c־רגולרי $|L| = n$, כך שהוא $((1-\varepsilon)c, \delta)$־אקספנדר עבור איזשהוא $\delta > 0$ בלתי תלוי ב־n.

נדלג על הוכחת המשפט ־ היא משתמשת ברנדומיות.

המשפט המרכזי שלנו להיום:

[5] ההגדרה שונה מעט מזו שמופיעה בסמינר של גרפים מרחיבים, אולם יתכן וניישב זאת מאוחר יותר.

משפט 3.8 אם $X=(L,R,E)$ גרף דו צדדי c־רגולרי, $|L|=n,\ |R|=m$ הוא (γ,δ) אקספנדר עם $\gamma>\frac{c}{2}$, אזי X נותן קוד עם:

$$rate\geq\frac{n-m}{n}$$

ומרחק מנורמל לפחות δ, כלומר $dist\left(C\right)\geq\delta n$, כלומר קיבלנו קוד טוב.

נשים לב כי התכונה של ה־$rate$ היא טריוויאלית, כי מספר המשוואות הוא m, לכן מרחב הפתרונות הוא $n-m$, וחלוקה ב־n מנרמלת כנדרש.

למה 3.9 לכל $S\subseteq L$ עם $|S|<\delta n$,

$$\left|\Gamma_{unique}\left(S\right)\right|\geq\left(2\gamma-c\right)\left|S\right|$$

למעשה הלמה הזו חזקה יותר ממה שהיינו צריכים ־ לכל קבוצה שכזו יש שכן שנוגע בדיוק פעם אחת (במקום קיום כזה שנוגע מספר אי זוגי של פעמים), והיא תגרור:

$$dist\left(C\right)\geq\delta n$$

הוכחה: אם $|S|<\delta n$, אז $\left|\Gamma\left(S\right)\right|\geq\gamma\left|S\right|$: המספר הטוטלי של הקשתות היוצא מ־S הוא $c\cdot|S|$. לכן המספר הממוצע שרואה כל שכן ב־R מתוך S הוא: $\frac{c\cdot|S|}{|\Gamma(S)|}$. אזי:

$$\frac{c\cdot\left|S\right|}{\left|\Gamma\left(S\right)\right|}\leq\frac{c\cdot\left|S\right|}{\gamma\left|S\right|}<\frac{c\cdot\left|S\right|}{\frac{c}{2}\cdot\left|S\right|}=2$$

כלומר בממוצע שכן של S מצד ימין רואה פחות מ־2 איברים ב־S, ולכן קיים $y\in R$ כך ש־y רואה איבר יחיד מ־S, דהיינו $\left|\Gamma_{unique}\left(S\right)\right|\neq\phi$.

ביתר דיוק, אם נסמן ב־a את מספר שכני S שרואים את S בדיוק פעם אחת: $a=\left|\Gamma_{unique}\left(S\right)\right|$, וב־$b$ את מספר שכני S הרואים את S יותר מפעם אחת. אזי:

$$a+2b\leq c\cdot\left|S\right|$$

וכמו כן:

$$a+b\geq\gamma\cdot\left|S\right|$$

שכן $\left|\Gamma\left(S\right)\right|=a+b$. משני אי השיוויונות האלו נקבל:

$$\begin{aligned}&a\geq\gamma\cdot\left|S\right|-b,\ b\leq\frac{c\cdot\left|S\right|-a}{2}\\&\Rightarrow a\geq\gamma\left|S\right|-b\geq\gamma\cdot\left|S\right|-\frac{c}{2}\left|S\right|+\frac{a}{2}\\&\Rightarrow\frac{a}{2}\geq\left(\gamma-\frac{c}{2}\right)\cdot\left|S\right|\end{aligned}$$

כנדרש. ■

עד כאן הכל טוב ויפה, אבל נרצה שה־$rate$ ישאר לינארי. הצורה שהבטחנו היא נחמדה אבל היא לא לגמרי מספקת - אם היא תהיה ע"י גרף מקרי, "החלפנו חמור בסוס" - יכולנו למצוא קודים מקריים טובים, ולא קודים מפורשים.

כאן יש בעיה עדינה אליה נחזור בהמשך ושהיא מעניינת בני עצמה - יש גרפים אקספנדרים טובים מאוד, אבל באופן מתסכל במיוחד, קודים שניתן לבנות ע"י גרפי רמנוג'אן (אופטימליים מבחינת ערכים עצמיים) - גרפים שיש להם בניות לא טריוויאליות, מגיעים למצב שהאקספנשן שמקבלים מהם הוא $\frac{c}{2}$ ממש, ולא גדול מהם (לפחות אנחנו לא יודעים להוכיח אחרת) כפי שאנחנו צריכים בשביל קודים טובים...

עד היום בקורס לא עסקנו בשאלות של $encoding$ ו־$decoding$. את חלק מהמשיכה של האנשים למאמר שציינו מ־98' נראה בשיעור הבא - בקוד שכזה יש תהליך מציאת השכן הקרוב ביותר שהוא מאוד מהיר - לינארי ב־n. 24/12/2012

שיעור חסר - יושלם בהקדם... 1/1/2013

והיום - השיעור הכי מעניין בקורס!

יהי X גרף l־רגולרי קשיר על n קודקודים עם ע"ע של $A = A_X$ מטריצת השכנות:

$$l = \lambda_0 > \lambda_1(X) \geq ... \geq \lambda_{n-1}(X) \geq -l$$

תהא Y תת־קבוצה של $V(X)$ ו־$G(Y)$ הגרף הנפרש ע"י Y ב־x, ז"א קשתותיו הן כל הקשתות של X ששתי נקודת הקצה ב־Y. נסמן:

$$L = \sum_{y \in Y} \frac{deg_{G(Y)}(y)}{|Y|}$$

כלומר ממוצע הדרגות של הקודקודים ב־y. ברור כי $L \leq l$. אזי, אם $L > \lambda_1(X)$, אזי $|y| \geq l - \frac{\lambda_1(X)}{l-\lambda_1(X)} \cdot |X|$.

הגדרה 3.10 קוד $C = (n,k,d)_{\mathbb{F}_q}$, ז"א תת מרחב של $\mathbb{F}_q^n$ ממימד k נקרא $LDPC$ (=low density parity check) אם יש מערכת של משוואות לינאריות המגדירות את C כתת מרחב של $\mathbb{F}_q^n$ שלכולן משקל $Hamming$ חסום מלמעלה ע"י קבוע (בלתי תלוי ב־n).

נציין כי קודים ציקליים ו־$LDPC$ לא יכולים להיות טובים.

טענה 3.11 C הוא $LDPC$ אמ"מ קיים $M \in \mathbb{N}$ קבוע, כך ש:

$$\begin{aligned} C^{\perp} &= \left\{ \beta \in \mathbb{F}_q^n \middle| \, \beta \cdot \alpha = 0 \ \forall \alpha \in C \right\} \\ &\beta = (b_1, ..., b_n), \ \alpha = (a_1, ..., a_n), \ \beta \cdot \alpha = \sum b_i \cdot a_i \end{aligned}$$

נפרשת ע"י וקטורים שמשקלם $\geq M$.

הוכחה: ברור! (חושבים על הדואלי כמשוואות המגדירות את C). ■

החשיבות של ה־$LDPC$ היא גם מעשית וגם תיאורתית - אם הקוד מאוד ארוך והגיע אלינו מילה, ונרצה לבדוק אם היא טובה, נצטרך לבדוק אם היא יושבת בתוך מרחב הקוד, כלומר מקיימת את המשוואות. דהיינו, לקחת את הוקטור α ולהכפילו במכפלה פנימית עם β. כלומר, נעדיף שב־β יהיו כמה שיותר אפסים, ואז מהמילה שמגיעה נצטרך לבדוק פחות ביטים, וכך בדיקת השגיאה תהיה הרבה יותר מהירה.

הראשון שדיבר על קודים טובים שהם $LDPC$ הוא גלאגר - אולם הוא בנה קודים כאלה רק בשיטות רנדומיות. כלומר, לקח משוואות חסומות אבל רנדומיות, והראה שבהסתברות טובה הוא מקבל קוד טוב.

המשפט הבא הוא פריצת דרך - הרבה שנים לא ידעו אם אפשר לקבל קוד שכזה באופן מפורש, עד להוכחת המשפט הזה:

משפט $Sipser-Spilman\,(98)$ **- בניה מפורשת של קודים** $LDPC$ **טובים**

הבניה יהא X גרף l-רגולרי על m קודקודים (נחשוב על l קבוע ו-$m\leftarrow\infty$). נמספר הקשתות היוצאות מ-v כ-$e_1(v),...,e_l(v)$.

יהא $B\subseteq\mathbb{F}_2^l$ **"קוד"** (=תת-מרחב) **קטן"** (הוא חד פעמי - נבחר פעם אחד ולתמיד) עם $rate=r_0=\frac{dimB}{l}$ ומרחק מנורמל $\delta_0=\frac{dist(B)}{l}$.

נגדיר עכשיו "קוד גדול" כתת מרחב של $\mathbb{F}_2^{E(X)}=\{f:E(X)\to\mathbb{F}_2\}$ באופן הבא:

$$C(X,B)=C=\left\{f\in\mathbb{F}_2^{E(X)}\middle|\,(f(e_v(1)),...,f(e_v(l)))\in B\ \forall v\in V(X)\right\}$$

כלומר לכל קודקוד v, <u>המבט המקומי</u> של f ב-v נמצא ב-B.

משפט 3.12 C הוא $\left(n=\frac{ml}{2},k,d\right)$-קוד, כאשר:

1.
$$rate(C)=\frac{k}{n}\geq 2r_0-1$$

2. אם $\delta_0>\lambda(X)$ (כאשר $\lambda(X)=\frac{\lambda_1(X)}{l}$).

אזי

$$\delta(C)=\frac{d}{n}\geq\left(\frac{\delta_0-\lambda(X)}{1-\lambda(X)}\right)^2$$

מסקנה 3.13 אם יש $B\subseteq\mathbb{F}_2^l$ עם $rate=r_0>\frac{1}{2}$ ומרחק מנורמל δ_0, ומשפחה של גרפים l-רגולריים $\{X_i\}_{i=1}^{\infty}$ עם m_i קודקודים ו:

$$\frac{\lambda_1(X_i)}{l}<\delta_0-\varepsilon\ \forall i$$

אזי $C_i=C(X_i,B)$ היא משפחה של קודים $LDPC$ טובים. מדוע?

טובים כמסקנה מיידית מהמשפט, שכן ה-$rate\geq 2r_0-1$, ואם $r_0>\frac{1}{2}$, $rate>0$ באופן בלתי קבוע, וכן אם $\lambda(X)<\delta_0$, $\delta(C)$ גם חסום מלמטה ע"י מספר חיובי.

הם $LDPC$, כי המשוואות המגדירות את B מחזיקות לכל היותר l ביטים, והקוד ה"גדול" מוגדר ע"י הרבה מאוד משוואות (מערכת לכל קודקוד) שאורכם לכל היותר l.

הוכחת המשפט: **הוכחה:** :

1. n = מימד המרחב = מספר הקשתות = $\frac{m\cdot l}{2}$. מספר המשוואות המגדירות את C הוא $m\cdot(l-dimB)$, ולכן

$$k = dimC \geq n-(m\cdot(l-dimB)) = \frac{m\cdot l}{2} - m\cdot l + m\cdot \overbrace{l\cdot r_0}^{dimB} = m\cdot l\left(r_0-\frac{1}{2}\right)$$

$$\Rightarrow \frac{k}{n} \geq \frac{m\cdot l\left(r_0-\frac{1}{2}\right)}{\frac{m\cdot l}{2}} = 2r_0 - 1 \overbrace{>}^{r_0>\frac{1}{2}} 0$$

2. תהא $f\in C$ ז"א f פונקציה על קשתות הגרף X, ונניח Z-קבוצת הקשתות הנשענת על f:

$$Z = \{\, e\in E(x) |\, f(e)\neq 0\}$$

ותהא Y קבוצת הקודקודים הנשענים על Z, זאת אומרת:

$$y\in Y \Leftrightarrow \exists e\in Z \ s.t.\ e=(y,x)$$

נשים לב שאם $y\in Y$, אזי: $0\neq f_y\in B$.

$$wt(f_y)\geq \delta_0\cdot l > \lambda(X)\cdot l$$

נשים לב כי מכאן נקבל כי

$$\forall y\in Y,\ deg_{G(Y)}(y) > \lambda_1(X)$$

זה גורר שהדרגה הממוצעת של Z, וקל וחומר של L - $G(Y)$, ו-$L>\lambda_1(X)$. על פי הלמה:

$$|Y| > \frac{L-\lambda_1(X)}{l-\lambda_1(X)}|X|$$

כמו כן, $supp(f)\geq \frac{|Y|}{2}$. נקבל:

$$|Z| \geq \frac{1}{2}\frac{\delta_0\cdot l-\lambda_1(X)}{l-\lambda_1(X)}|X|$$

יש כאן בעיה של קבוע, אולי נצליח לעדכן בהמשך...

■

3.2 קודים סימטריים

הגדרה 3.14 קוד $C\leq \mathbb{F}_2^n$ יקרא סימטרי אם קיימת חבורה $H\geq Sym(n)$ הפועלת טרנזיטיבית על $\{1,...,n\}$ (ולכן H פועלת על $\mathbb{F}_2^n$ באופן ברור), כך ש-C אינווריאנטי תחת H.

דוגמא: קוד ציקלי.

משפט 3.15 (של אלכס לובוצקי וטלי קאופמן מהשנה שעברה) יש קודים טובים $LDPC$ וסימטריים.

זאת בניגוד לקודים ציקליים. משפט זה נגד את התפיסה של תורת הקודים שהיתה קודם לכן - זאת מכיוון וכל הקודים הטובים הושגו מרנדומיזציה, ואילו המשפט מציג בניה מפורשת. לקודים שנמצאו במשפט הזה היו עוד כמה תכונות טובות נוספות.

4 קודים בדיקים מקומית (LTC - Locallty Testable Codes)

8/1/2013

נרצה יכולת לדעת מהר אם וקטור הוא בקוד או רחוק מהקוד. ובאופן פורמלי:

הגדרה 4.1 עבור $C \subseteq \{0,1\}^m$ קוד באורך n, נאמר כי C הוא $q-LTC$, אם קיים אלגוריתם אקראי[6] (tester) שבהנתן $f \in \{0,1\}^m$ קורא q ביטים אקראיים מתוך f ופועל באופן הבא:

- אם $f \in C$, עונה "כן" (בהסתברות 1).
- אם $dist(f,C) = \delta$, עונה "לא" בהסתברות $> \alpha \cdot \delta$ עבור $\alpha > 0$ קבוע כלשהוא.

נשאל, האם בכלל קיימים קודים $q-LTC$ עבור $q = 3$ (q קבוע). התוצאה הראשונה בתחום הזה היתה של $Blum, Luby, Rubinfeld$, והיא:

משפט 4.2 (BLR) קוד $Hadamard$ הוא $3-LTC$.

ה־α שהם השיגו היתה $\frac{2}{9}$. מאוחר יותר בעזרת אנליזת פוריה שיפרו ל־1. לאחר מכן הוכיחו כי α יכול להיות גדול מ־1.

תזכורת: קוד $Hadamard$ מוגדר באופן הבא:

$$C = \left\{ f : \mathbb{F}_2^m \to \mathbb{F}_2 \middle| \, f = \sum_{i=1}^{m} a_i x_i, \; a_i \in \mathbb{F}_2 \right\}$$

כל מילה של C היא הערכה של פונקציה לינארית כלשהיא ב־m משתנים על כל ה־$domain$ שלה. דהיינו, $C = \left[2^m, m, 2^{m-1}\right]$.

כלומר, זהו קוד שהוא רחוק מלהיות טוב.

תזכורת: Had הוא קוד דואלי ל־$BCH_2(m,1)$.

שאלה פתוחה חשובה:

האם יש קודים טובים שהם $q-LTC$ עבור q קבוע?

ביתר השיעור, נוכיח את טענת BLR. על מנת להוכיח את המשפט, תחילה יש להגדיר את ה־$tester$.

טסטר בחר $x, y \in_R \{0,1\}^m$ (בצורה אוניפורמית). החזר 1 אמ"מ $f(x) + f(y) = f(x+y)$.

כלומר חושבים על מילת הקוד בתור משהו מאוד ארוך - 2^m, בוחרים זוג אקראי, וזוג זה יגדיר לנו קואורדינטה שלישית.

ברור כי $q = 3$ מהגדרת הטסטר. כמו כן, ברור כי אם f היתה פונקציה לינארית, אז הוא יתקבל בהסתברות 1. כלומר, אם $f \in C$, f מתקבלת בהסתברות 1. נותר רק להוכיח:

למה 4.3 אם $dist(f,C) = \delta$, אז הטסטר המוגדר מעלה דוחה בהסתברות $> \frac{2}{9} \cdot \delta$.

[6] כלומר אלגוריתם שמשתמש בפונקציית הסתברות כלשהיא שקשורה לקוד.

לשם ההוכחה, נמשיך עם פיתוח נוסף.
נסמן:

$$\eta = \underset{x,y\in_R\{0,1\}^m}{Prob}\left(f\left(x\right)+f\left(y\right)\neq f\left(x+y\right)\right)$$

דהיינו η היא הסתברות הדחיה של הטסט.
נרצה להגדיר עכשיו פונקציה בשם פונקציית רוב - היא תסתכל לכל x על כל הטסטים שעוברים בקואורדינטה הזו, ותחליט מה הוא צריך להיות כדי שרוב הבדיקות יהיו חיוביות. ובאופן פורמלי:

הגדרה 4.4 בהנתן f, נגדיר פונקציית רוב g באופן הבא:

$$\forall x\in\{0,1\}^m\ \ g\left(x\right):=\underset{y\in\{0,1\}^m}{maj}\left(f\left(x+y\right)+f\left(y\right)\right)$$

ההוכחה תנבע משתי הטענות הבאות:

טענה 4.5 $dist\left(g,f\right)\leq 2\eta$.

טענה 4.6 :

1. אם $\eta<\frac{2}{9}$, אזי $g\in C$.
2. שתי הטענות מעלה $\Leftarrow$ משפט BLR

הוכחה: נשים לב כי אם $\eta\geq\frac{2}{9}$, דוחים בהסתברות $\leq\frac{2}{9}\cdot\delta$ לכל $0<\delta\leq 1$ (ברור, ללא שימוש בטענות).
אם $\eta<\frac{2}{9}$, לפי הטענה השניה כי $g\in C$, ועל כן

$$\begin{aligned}\delta &= dist\left(f,C\right)\leq dist\left(f,g\right)\overset{1st\ claim}{\leq}2\eta\\ \Rightarrow\eta &\geq \frac{\delta}{2}\\ \Rightarrow\eta &\geq min\left\{\frac{2}{9}\delta,\frac{\delta}{2}\right\}\geq\frac{2}{9}\delta\end{aligned}$$

■

כפי שציינו, בהמשך שיפרו את היחס $\frac{2}{9}$, ואולם השיפורים ניתחו את אותו הטסטר - כלומר, אנו עוד רחוקים מלהבין את ההתנהגות שלו...
כעת, נוכיח את טענה 1: **הוכחה:** נגדיר:

$$\begin{aligned}Bad &= \left\{x\in\{0,1\}^m\ \middle|\ \underset{y\in_R\{0,1\}^m}{Pr}\left[f\left(x\right)+f\left(y\right)\neq f\left(x+y\right)\right]\geq\frac{1}{2}\right\}\\ &\Rightarrow\ \forall x\notin B\ f\left(x\right)=g\left(x\right)\end{aligned}$$

כלומר עבור $x\notin B$ רב הטסטים מצליחים, ועל x שכזה f,g מסכימות, ולכן:

$$dist\left(f,g\right)\leq\frac{\left|Bad\right|}{\left|\{0,1\}^m\right|}$$

מצד שני:

$$\eta := \underset{x,y\in_R\{0,1\}^m}{Pr}\left[f\left(x\right)+f\left(y\right)\neq f\left(x+y\right)\right]$$

אם $x\in B$, אז מחצית או יותר מהטסטים מעליו נכשלים, דהיינו $\eta\geq\frac{1}{2}\frac{|Bad|}{2^m}$. לכן בסה"כ:

$$dist\left(f,g\right)\leq\frac{|Bad|}{|\{0,1\}^m|}\leq 2\eta\Rightarrow dist\left(f,g\right)\leq 2\eta$$

■

ולסיום, נוכיח את הטענה השניה: **הוכחה:** רוצים להראות שאם $\eta<\frac{2}{9}$, אז $g\in C$. נראה זאת ע"י כך שנוכיח כי לכל $x,z\in\{0,1\}^m$ מקיימים:

$$g\left(x\right)+g\left(z\right)=g\left(x+z\right)$$

שאן אם פונקציה מקיימת את השיוויון הזה, הפונקציה היא לינארית, ולכן בפרט בקוד.

נראה כי פונקציית הרוב שהגדרנו היא למעשה פונקציית רוב מוחץ - כלומר עבור כל x, מספר הטסטים שעוברים הוא "מאוד גדול". זוהי אסטרטגיה רווחה בקרב הוכחות של טסטבילויות.

מהגדרת g ידוע:

$$\gamma_x := \underset{y\in\{0,1\}^R}{Pr}\left[g\left(x\right)=f\left(g\right)+g\left(x+y\right)\right]\geq\frac{1}{2}$$

נראה כי g היא למעשה פונקציית רב מוחץ, כלומר, לכל $x\in\{0,1\}^m$:

$$\gamma_x>\frac{2}{3}$$

לשם כך, נבחן את בהסתברות הבאה:

$$\underset{y_1,y_2\in\{0,1\}^m}{Pr}\left[f\left(y_1\right)+f\left(x+y_1\right)=f\left(x+y_2\right)+f\left(y_2\right)\right]\overbrace{=}^{(*)}\gamma_x^2+\left(1-\gamma_x\right)^2$$

שכן המאורע מתרחש כאשר או ששניהם מסכימים עם הרב, או ששניהם לא (ישירות מההגדרה). נוכל לכתוב זאת גם כך:

$$\underset{y_1,y_2\in\{0,1\}^m}{Pr}\left[f\left(y_1\right)+f\left(x+y_2\right)=f\left(x+y_1\right)+f\left(y_2\right)\right]$$

נסתכל על הסתברות נוספת (מיד נקשר להסתברות הקודמת שניתחנו:

$$\underset{y_1,y_2\in\{0,1\}^m}{Pr}\left[\overbrace{f\left(y_1\right)+f\left(x+y_2\right)\neq f\left(x+y_1+y_2\right)}^{A}\right]$$

נשים לב שלמרות שיש כאן שני y-אים שונים, אנו מסתכלים כאן על טסט אקראי (שכן x קבוע). על כן ההסתברות הזו $=\eta$.

באופן דומה:

$$\underset{y_1,y_2\in\{0,1\}^m}{Pr}\left[\overbrace{f\left(x+y_1\right)+f\left(y_2\right)\neq f\left(x+y_1+y_2\right)}^{B}\right]=\eta$$

לכן אם התרחשו לא A ולא B, הטסט צלח, ואז יש שיוויון בין שני הצדדים הימניים בשני האירועים, כלומר:

$$\underset{y_1,y_2\in\{0,1\}^m}{Pr}\left[f\left(y_1\right)+f\left(x+y_2\right)=f\left(x+y_1\right)+f\left(y_2\right)\right]\geq 1-2\eta$$

ועל פי $(*)$:

$$\gamma_x^2+\left(1-\gamma_x\right)^2\geq 1-2\eta>\frac{2}{5}$$

מכיוון ואנו מניחים כי $\eta<\frac{2}{9}$, נקבל כי:

$$\gamma_x>\frac{2}{3}$$

נקבע $x,z\in\{0,1\}^m$ כלשהם. מכיוון ו־$\gamma_x>\frac{2}{3}$ לכל x:

$$\underset{y\in\{0,1\}^m}{Pr}\left[g\left(x\right)\neq f\left(y\right)+f\left(x+y\right)\right] < \frac{1}{3} \quad (1)$$

$$\underset{y\in\{0,1\}^m}{Pr}\left[g\left(z\right)\neq f\left(y\right)+f\left(z+y\right)\right] < \frac{1}{3} \quad (2)$$

$$\underset{y\in\{0,1\}^m}{Pr}\left[g\left(x+z\right)\neq f\left(y\right)+f\left(x+y+z\right)\right] < \frac{1}{3} \quad (3)$$

$$\Rightarrow \underset{y\in\{0,1\}^m}{Pr}\left[g\left(x+z\right)\neq f\left(y+z\right)+f\left(x+y\right)\right] < \frac{1}{3} \quad (4)$$

שכן שתי השורות האחרונות שוות.

מכיוון וסכום ההסתברויות של המאורעות (הרעים) שבחנו קטן ממש מ־1, קיים $y\in\{0,1\}^m$ שמקיים את שלושת השיוויונות, דהיינו :

$$g\left(z\right)+g\left(x\right)\overbrace{=}^{(1),(2)}f\left(y\right)+f\left(x+y\right)+f\left(y\right)+f\left(y+z\right)\overbrace{=}^{(3)}g\left(x+z\right)$$

כלומר

$$g\left(x\right)+g\left(z\right)=g\left(x+z\right)$$

וזה מתקיים לכל $x,z\in\{0,1\}^m$, ולכן $g\in C$, כנדרש! ■

וכאן למעשה סיימנו את הוכחת המשפט.

נשים לב כי מכאן אנו מקבלים כי קוד Had הוא קוד $LDPC-3$ - הוא מוגדר ע"י השלשות של הטסטר. אנחנו בחרנו להסתכל על כל השלשות, ולאו דווקא על המספר

המינימלי שאפשר להסתכל עליהן. אולי יש קוד שמספיק להסתכל על המספר המינימלי? יש משפט שאומר שקוד שכזה, כלומר קוד $LDPC$ שמרחב הקוד הדואלי שלו קטן מ־n^2 (מרחב השלשות), אינו LPC, כלומר יש הכרח ביתירות במספר האילוצים. קודים רנדומיים למשל הם גם לא LPC.

בפעם הבאה ננסה להבין את רעיון ההוכחה הזו, והאם אפשר לגזור ממנה רעיון כללי לקריטריון כללי שגורר LTC ש"יתפוס" הרבה יותר קודים. 15/1/2013

בשביל מציאת קריטריון שכזה, נפתח בהגדרה:

הגדרה 4.7 נאמר שלקוד $C \subseteq \left\{F^2 \to F\right\}$ **אפיון א־פורמלי**, אם קיים $m \leq k$, $V \subsetneq F^k$ וקיימות k פונקציות לינאריות:

$$1 \leq i \leq k,\ l_i : \{F^n\}^m \to \{F^n\}$$

כך שלכל $y_1, ..., y_m \in F^n$ מתקיים:

$$l_i\left(y_1, ..., y_m\right) = \sum_{j=1}^{m} a_j y_j$$

וכמו כן נניח ש־ $l_i\left(y_1, ..., y_n\right) = y_i$ עבור $1 \leq i \leq m$, כך ש:

$$f \in C \Leftrightarrow \forall y_1, ..., y_m \in F^n,\ \left(f\left(l_1\left(y_1, ..., y_m\right)\right), ..., f\left(l_k\left(y_1, ..., y_m\right)\right)\right) \in V$$

הגדרה מסובכת ־ ננסה להסביר אותה בעזרת דוגמא ־ ל־Had יש אפיון 3־פורמלי עבור $m = 2$:

$$\begin{aligned}
&l_1\left(y_1, y_2\right) = y_1 \\
&l_2\left(y_1, y_2\right) = y_2 \\
&l_3\left(y_1, y_3\right) = y_1 + y_2 \\
&V = \left\{(011), (110), (101), (000)\right\}
\end{aligned}$$

ונזכור כי $f \in Had$ אמ"מ

$$\forall x, y\ 0 = f\left(x\right) + f\left(y\right) + f\left(y + x\right)$$

הגדרה 4.8 נאמר שלקוד $C \subseteq \{F^n \to F\}$ יש **אפיון k־פורמלי, 2 בת"ל**, אם לכל $2 \leq i \leq k$ הוא בת"ל ב־l_1.

כלומר, אם קבענו את l_1 נרצה ששאר הקואורדינטות לא יקבעו גם כן.

הערה 4.9 כל קוד $C \subseteq \{F^n \to F\}$ שהינו בעל אפיון k־פורמלי והוא אינווריאנטי תחת חבורה אפינית, הוא בעל איפיון 2־בת"ל, כאשר C הוא אינווריאנטי תחת חבורה אפינית אם לכל $f \in C$ ולכל $A_{n\times n}, b$ מתקיים $f\left(Ax + b\right) \in C$.

נשתמש בהערה זו בהמשך ההרצאה על מנת לקבל אפיון 2 בת"ל ־ בעצם זה מראה שהרבה פעמים מקבלים אפיון זה "בחינם" באופן טבעי.

מסקנה 4.10 קודי RM הם בעלי אפיון k-פואמלי 2 בת"ל עבור k קבוע כלשהוא.

משפט 4.11 $C \subseteq \{F^n \to F\}$ בעל אפיון k-פורמלי 2-בת"ל הוא $K-LTC$ ע"י טסטר שבהנתן f בוחר בהתפלגות אחידה $y_1,...,y_m \in_R \{F^n\}$, ובודק:

$$(f(l_1(....)),...,\ f(l_k(...))) \in V$$

אם $f \in C$, f יתקבל בהסתברות 1 (מהגדרת האפיון), ואם $d(f,C) = \delta$, f נבחר בהסתברות $< \delta \cdot \frac{1}{(2k+1)(k-1)}$.

בעצם, האפיון "אומר לנו באיזה קואורדינטות להסתכל".
עברו 15 שנה בין המשפט שראינו בשיעור הקודם למשפט הזה, עד אז הוכיחו LTC עבור קודים כלליים.

הגדרה 4.12 נגדיר את **הסתברות הדחיה של הטסט** להיות:

$$\eta = \underset{y_1,...,y_m \in_R F^n}{Prob}[(f(l_1(y_1,...,y_n)),...,f(l_k(y_1,...,y_n))) \notin V]$$

הגדרה 4.13 נגדיר פונקציית רוב יחסית ל-$f: F^n \to F$ באופן הבא:

$$x \in F^n \ g(x) = \underset{y_1,...,y_m \in_R F^n}{Prob}\left[S_C^f(x,y_2,...,y_m)\right]$$

כאשר $S_C^f(x,y_2,...,y_m) = \alpha$ אמ"מ $V \ni (\alpha, f(l_2(x,y_2,...,y_m)),...,f(l_k(x,y_2,...,y_m)))$ (כלומר, אם אפשר "לתקן" אותו להיות מילה חוקית - ו-α יחיד, אחרת לא היה אילוץ על אותה הקואורדינטה, כלומר היה אפיון $k-1$ פורמלי), אחרת $S_C^f(x,y_2,...,y_m) = \perp$.

הערה 4.14 דהיינו, אם $f \in C$, $\alpha = g$.

הערה 4.15 נשים לב כי:

$$\eta = \underset{x,y_2,...,y_m \in F^n}{Pr}\left[f(x) \neq S_C^f(x,y_2,...,y_m)\right]$$

ההוכחה היא באופן דומה להוכחה שראינו בשיעור הקודם - תחילה, 3 למות:

למה 4.16

$$\underset{y_2,...,y_m \in F^n}{Pr}\left[g(x) = S_C^f(x,y_2,...,y_n)\right] \geq 1 - 2(k-1)\cdot\eta$$

למה 4.17

$$dist(f,g) \leq 2\eta$$

למה 4.18 אם $\eta < \frac{1}{(2k+1)(k-1)}$, אזי $g \in C$

נוכיח כי שלוש הלמות גוררות את המשפט: **הוכחה:** אם $\eta < \frac{1}{(2k+1)(k-1)}$, אז

$$dist\left(f,g\right) \overset{third\ lemma}{\leq} dist\left(f,g\right) \overset{seond\ lemma}{\leq} 2\eta$$

ומכאן:

$$\eta \geq min\left\{\frac{1}{\left(2k+1\right)\left(k-1\right)}, \frac{\delta}{2}\right\} \geq \frac{\delta}{\left(2k+1\right)\left(k-1\right)}$$

■

לב העניין הוא הלמה הראשונה - נוכיח אותה: **הוכחה:**

$$Pr\left[g\left(x\right) \neq \underset{y_2,...,y_m \in_R F^n}{S_C^f\left(x,y_2,...,y_m\right)}\right] \leq Pr\left[\underset{y_2,...,y_m \in_R F^n,\ z_2,...,z_m \in_R F^n}{S_C^f\left(x,y_2,...,y_m\right) \neq S_C^f\left(x,z_2,...,z_m\right)}\right]$$

כי ההסתברות להתנגשות היא גדולה יותר מההסתברות לשכיח.
נראה כי:

$$Pr\left[S_C^f\left(x,y_2,...,y_m\right) \neq S_C^f\left(x,z_2,...,z_n\right)\right] \leq 2\left(k-1\right)\eta$$

נביט במטריצה:

$$\begin{pmatrix} x & y_2 & \cdots & y_m & ? \\ z_2 & & & & \\ \vdots & & & & \\ z_m & & & & \\ ? & & & & \end{pmatrix}$$

ואת שאר הקואורדינטותיש נשלים לאילוצים.
נתחיל מהשורה הראשונה והעמודה הראשונה - שם האילוצים יהיו $l_{m+1}\left(x,y_2,...,y_m\right)\cdots l_{m+1}\left(x,y_2,...,y_m\right)$, וכנ"ל לגבי העמודה הראשונה, רק עם z במקום y.
לאחר מכן, נבחר ריבוע $\gamma_{i,j}$ אקראי בתוך הריבוע השמאלי העליון, וגם אותו נשלים לאילוצים באותו אופן.
לאחר מכן -

$$M_{i,j} = l_j\left(M_{i,1},...,M_{i,m}\right)$$

ובאופן דומה

$$M_{i,j} = l_i\left(M_{1,j},...,M_{m,j}\right)$$

ומהלינאריות שני הביטויים מעלה שווים. אז אפשר להסתכל על כל n-יהף ולהשלים אותה בצורה תיקנית.
כל שורה פרט לשורה הראשונה, וכל עמודה פרט לעמודה הראשונה, מתארות אילוץ אקראי (הראשונות לא, כי x לא אקראי, אבל השאר כן). נביט ב:

$$N = \begin{pmatrix} S_c^f(x, y_2, ...y_m) & & \\ & & f(M_{i,j}) \\ & & \end{pmatrix}$$

כאשר ב־$f(M_{i,j})$ $k-1$ שורות. אם כך, ההסתברות שקיימת עמודה (לא ראשונה) או שורה (לא ראשונה) ב־N שאיננה שייכת ל־V היא לכל היותר $2(k-1)\eta$, כלומר בהסתברות $1-2(k-1)\eta$ כל שורה וכל עמודה (פרט לראשונות) שייכת ל־V.

נחשוב על N במילה בטנזור פרודקט $V \times V$. מתכונות של tensor product, אם המרחק של V הואלפחות 2, אזי כל תת מטריצה בגודל $(k-2+1) \times (k-2+1)$ שבה כל שורה וכל עמודה ניתנות להשלמה למילה של V, כזו מטריצה ניתן להשלמה יחידה של מילה ב־$V \times V$, כלומר במקרה:

$$S_C^f(x, y_2, ..., y_m) = S_C^f(x, y_2, ..., y_m)$$

■

חומר לקריאה נוסף בנושא - במאמר של טלי ו־Madhu Sudan:

Algebraic Property Testing: The Rule of Invariance